Project acronym:	IRISS
Project title:	Increasing Resilience in Surveillance Societies
Objective:	To investigate societal effects of different surveillance practices from a multi-disciplinary social science and legal perspective.
Start date of project:	01 February 2012
Duration:	36 months

Deliverable D3.2: Surveillance Impact Report

Coordinator:	Open University (OU)
Dissemination level:	PU
Deliverable type:	Report
Version:	1
Submission date:	12 June 2014

List of Authors

Executive Summary	Kirstie Ball, Keith Spiller
Chapter 1	Kirstie Ball, Keith Spiller
Chapter 2	Kirstie Ball, Sebastien Dahm, Michael Friedewald, Antonella Galletta, Kerstin Goos, Richard Jones, Erik Lastic, Clive Norris, Charles Raab, Keith Spiller.
Chapter 3	Kirstie Ball, J Peter Burgess, Stine Bergersen, Rocco Bellanova, Alessia Ceresa, Chiara Fonio, Walter Peissl, Robert Rothman, Jaro Sterbik Lamina, Keith Spiller, Ivan Szekely, Beatrix Vissy
Chapter 4	Kirstie Ball, Wolfgang Bonß, Daniel Fischer, Gemma Galdon Clavell, Reinhard Kreissl, Chalres LeLeux, Alexander Neumann, Keith Spiller, William Webster, Nils Zurawski,
Chapter 5	Kirstie Ball, Keith Spiller
Policy Implications & Recommendations	Kirstie Ball

Acknowledgement: This deliverable is written as part of the IRISS project which received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement No. 285593.

Table of Contents

List of Abbreviations

ACPO – Association of Chief Police Officers

ANPR – Automatic Number Plate Recognition

BISZ – Inter-Bank Information Service Corporation

BOF – Back Office Facility

CIFE – Credit Institutions and Financial Enterprises

CCIS – Central Credit Information System

CTU – Counter Terrorism Unit

DPA – Data Protection Act

DP Code – Data Protection Code

DSK – Data Protection Commission

DVLA – Driver and Vehicle Licencing Agency

ETS – Electronic Toll System

FIT – Forward Intelligence Team

FMA – Financial Market Authority

FOI – Freedom of Information

FLHR – Flemish League of Human Rights

ICO – Information Commissioner's Office

IPOL – International Police Intelligence Department

KSV – Kreditschutzverband (Austrian Credit Protection Association)

NADC – National ANPR Data Centre

NDS – National Highway Company (Narodna Dialnicna Spolocnost – Slovakia)

NGO – Non Government Organisation

NPOIU – National Public Order Intelligence Unit

NW – Neighbourhood Watch

OBU – On-Board Unit

OeNB – Austrian National Bank

OFT – Office of Fair Trading

P-N – Pro-Nachbarn

RIPA – Regulation of Investigatory Powers

SIS – Schengen Information System

SIS – Slovak Information Service

TAM – Terrorism and Allied Matters

VRM - Vehicle Registration Mark

List of Tables, Figures and Boxes

Tables

Figures

Boxes

EXECUTIVE SUMMARY

This deliverable presents case studies of three surveillance practices across Europe: ANPR, Credit Scoring and Neighbourhood Watch. These practices were chosen because they represent different institutional surveillant relationships: between citizens and the state (ANPR), citizens and the private sector (Credit Scoring) and citizens and each other (Neighbourhood Watch). The report examines how democratic resilience can be increased in the face of these pervasive surveillance practices. The theoretical premise for the case study is that while surveillance practices can be deployed to counter threats and risks and to prevent harm occurring, they also create potentially harmful consequences. The reliance of surveillance practices on proprietary information infrastructures can make surveillance processes intransparent and unaccountable to democratic scrutiny. As the capacity to surveil bestows great power, it is of concern that this power is wielded responsibly, ethically and with due respect to the law and human rights. In this work package, the case studies concerned the extent to which the focal surveillance practices created harms or were controversial, and the extent to which they intersected with democratic practices of governance, participation and engagement.

Three case studies were examined in 11 different European countries. ANPR was examined in Belgium, Germany, Slovakia and the UK. Credit Scoring was examined in Austria, Hungary, Italy, Norway and the UK; Neighbourhood Watch was examined in Austria, Germany, Spain and the UK. The central finding is that increasing resilience to surveillance in Europe begins with increased public – and institutional - awareness of its harms and its benefits. For the watchers - those organizations in whose favour surveillance was deployed - surveillance produced several benefits. These benefits included better risk management and traffic law enforcement which has almost made the watchers immune to recognising that any harm may arise. Nevertheless, activist groups and the media have been working hard to highlight the harms associated with specific instances of ANPR (UK, Slovakia, Belgium), and Credit Scoring (UK, Norway) but changes in governance are also needed to limit the effect of those harms. The picture here is variable, as follows.

ANPR resulted in some harms against which resilient strategies need to be formulated. The case studies found evidence that use of ANPR had circumvented and breached the rule of law, compromised rights and had raised privacy issues. In the least regulated country, the UK, it had been found to affect detrimentally the right to protest and had deliberately been deployed in a racist way by police in Birmingham following Project Champion. However the situation in Slovakia extended the harms resulting from a surveillance practice. In an effort to avoid the economic losses imposed by road tolls, Slovakian truck drivers had taken to driving on smaller roads and affecting the quality of life for the villages which were located on those roads. In the ANPR case, with the exception of Germany, very low engagement of the public was evident because of a lack of consistent regulation and signage, low levels of general media coverage and low engagement of data protection regulators with the practice. In relation to ANPR, in respect of its very significant harms we observed different levels of governance which lagged behind technological capabilities. The first priority would be to harmonise governance with a European level directive. The gold standard developed in Germany, based on constitutional scrutiny and limitation of ANPR data collection would be a good starting point. Mandatory signage, enhanced DPA powers and the use of Privacy by Design in tendering processes for ANPR systems would perhaps feature in this directive.

The provision of figures proclaiming the effectiveness of ANPR systems in detecting crime should also be made available by law enforcement agencies.

The harms associated with credit scoring relate to administrative matters and highlight how this form of surveillance is explicitly part of a management process and hence subject to administrative errors. However evidence was also uncovered of bank and legal staff abusing their position in relation to this sensitive financial data (Austria, Hungary). Similarly its location in the commercial sector meant that some unscrupulous organizations exploited it to facilitate the lending money to customers who could ill afford it and were financially illiterate (UK). Overall this points to a problem with transparency and with the operation of the rule of law in relation to credit scoring (Italy, Hungary, Austria). The distributive justice aspects of credit scoring and its ability to delimit economic prosperity were noted in the UK and Norwegian cases particularly. With the exception of Norway and the UK, there was minimal public engagement and low awareness of the practice. The first issue to solve is the public's awareness of and access to their own credit scoring data. While this is widely available in the UK and Norway, this is not the case in Austria, Italy and Hungary. Increasing transparency and accountability of financial institutions in relation to credit scoring data again could be instantiated at European level. Other countries could learn from the Norwegian model, which places DPA at the heart of credit scoring and invests genuine powers in the courts to hear citizens' complaints about credit scoring practices. Following the credit crunch, demand for credit is now increasing across Europe and institutions should take this opportunity to inform consumers of their rights. Controversies associated with credit scoring appear in all of the case study countries, but in some cases the media have been slow to react, resulting in ill informed consumers and unaccountable, intransparent banks.

In the Neighbourhood Watch case studies, privacy was a relatively minor issue associated with the schemes' use of online and social media. The cultural and social significance of surveillance was far more powerful and generated strong sentiment towards it as a community safety idea (Austria, Germany, Spain). In these cases surveillance processes became controversial because as well as creating unhelpful links with the past, it was feared that they would present opportunities for extremists of all political colours. Indeed this was observed as a shock in the German and Spanish cases. The presence of NW-like organizations stigmatised particular spaces and focused on victimising those who were perceived as 'other' at that moment. It also challenged policing authorities who, at a community level, tread a fine line between too-little or too-much intervention, leading to a rise in feelings of security if crime appears to be increasing. Neighbourhood Watch is a special case in that, with the exception of the UK, it has developed outside the remit of law enforcement institutions. However the experience of NW in the case study countries is simultaneously an example of community resilience and community breakdown. In an attempt to create community safety its harms stem from frustration with 'the other' and insecurities in relation to community policing. The British example, with minimal regulation and a caring focus, shows how NW can succeed without the deep levels of mistrust and unpleasant associations which stem from authoritarian pasts. The community reaction Neighbourhood Watch in Austria, Germany and Spain represents how those societies have become resilient to the surveillance they suffered at the hands of authoritarian and fascist governments. Improved relations within communities as well as between communities and police would further strengthen this resilience. Frustrations with a low police presence as a result of funding cuts (among other things) point to how this surveillance practice is intertwined with public resourcing issues. Whilst it is inevitably difficult to prioritise resource

deployment in the current public financial climate, it is always important for police to be connected with the communities that they serve.

Overall the intersection between surveillance and democracy across the three case studies we have examined is varied. Patterns have emerged which are associated with historical, legal, political, social and institutional factors. To a greater degree than ever before, surveillance processes intersect with and constitute the way in which we get things done. As consumption, communication, security and even democracy is done in this way – we need to question how transparency and accountability re-organize themselves - which will enable alternatives to emerge.

CHAPTER ONE

INTRODUCTION

This deliverable reports on 14 case studies of three separate surveillance practices across Europe. These case studies were designed to interrogate the intersection between democratic activities and surveillance practices from the perspectives of both watcher and watched. There are some tensions inherent in the relationship between surveillance and democracy as outlined by Sewell and Barker (2006)[1]. Drawing on Haggerty and Samatas (2010)[2] we note a complex, multi-layered and sometimes fraught relationship between the two concepts. To use a straightforward definition, 'democracy involves a system of open procedures for making decisions in which all members have an equal right to speak and have their opinions count' (2010:1). Democracy is simultaneously an idea, a doctrine, a set of institutional arrangements and a way to relate to others: it describes forms of governing, participating and engaging. At times surveillance helps to facilitate democracy: it runs through the information infrastructures which, for example, help to target welfare at the most needy, facilitate democratic participation through voting and distribute public resources efficiently. However, surveillance can erode the institutional trust required for democratic governance. Fear of having one's opinions, movements or activities monitored can quash debate within targeted groups in both authoritarian, post authoritarian and in democratic societies. As citizens and consumers become more aware of how their actions and communications are monitored, surveillance can alter the forms and nature of public participation in all sorts of arenas.

[1] Sewell, G., & Barker, J. R. (2006). Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review*, *31*(4), 934-961.
[2] Haggerty, K. D., & Samatas, M. (Eds.). (2010). *Surveillance and Democracy*. London: Routledge.

Haggerty and Samatas (2010)[3] cite several ways in which surveillance challenges notions of democracy.

- New surveillance techniques and technologies tend to develop in the commercial realm, in response to commercially sensitive issues which are not subject to public scrutiny or political debate. Any regulation thus comes too late.
- Recent developments in public policy which mandate the extension and intensification of surveillance have occurred in response to a crisis where a poorly designed and sometimes draconian solution results.
- The public-private blurring which often accompanies extensions in government surveillance activities means that surveillance capacity which is developed in the private sector, while governed by law, is not always as publicly accountable as it might be.

One theoretical framework specific to surveillance studies attempts to chart the relationship between surveillance and democracy. Murakami Wood (2012)[4] attempts to map different state forms against the nature of information flow to characterise the different forms of surveillance society. He refers to a number of forms which are relevant in Europe. First, he argues that in democracies, three types of surveillance society would emerge in relation to low, medium and high information flow. He characterises democracy in terms of the strong rights frameworks under which they operate and which apply to all citizens.

Low information flow, Murakami Wood argues, produces an *Adiloptic Democracy*. Adiloptic, meaning 'blind seeing' describes a situation in which no information flows or information flow in obscured. This is a surveillance society characterised by opacity. There is a limited capacity for the state or corporations to surveil citizens, but citizens possess the ability, via a democratic rights framework, to know what information is held about them and how it is

[3] Ibid n.1
[4] Murakami Wood, D (2012) Integrating Surveillance into Theories of the State: Towards a Model of Surveillance Societies. Paper presented at the 5th Biannual Surveillance and Society Conference, University of Sheffield 2 – 3 April 2012.

processed. However these systems of redress are not needed because information processing is so minimal.

Medium information flow, it is argued, produces a *Synoptic Democracy.* Synoptic means 'all together seeing'. An accountable surveillance society is created. In the synoptic democracy there is a stronger bias towards the citizen in terms of their ability to hold the state to account via a strong rights framework. The ability of the state and corporations to collect data at will on the population is limited by constitutional and legal frameworks. Information and privacy is strongly regulated with strong civil protections in place. Murakami Wood argues that Germany and the Netherlands are contemporary examples of the synoptic democracy.

High information flow produces the *Perioptic Democracy.* Perioptic means 'all around seeing' and a surveillance society based on reciprocity is created. In the Perioptic Democracy there is a strong commitment to democracy in conditions of high information flow. The state maximises the amount of information it can collect but citizens also have access rights to that information. Murakami Wood notes that there is a strong sense of common interest in states run along these lines and cites Scandinavian countries, especially Sweden as indicative contemporary examples.

A further category of state he refers to is the Polyarchy, where power is dispersed among several large actors, such as the state and its various organs as well as the private sector. This, he argues, applies to some European States.

Under conditions of low information flow, *Adiloptic Polyarchies* emerge. These states are limited democratic states that do not depend on information to function. He argues that this may be because of constitutional restraints, which leaves this kind of state open to arbitrary actions and corruption. The state becomes very opaque in an adiloptic polyarchy.

Medium information flow, produces *Oligoptic Polyarchies*. Oligoptic refers to the idea that a few can see, producing a regulated surveillance society. In these kinds of society the state processes, uses and disseminates information but has a lot of choice in terms of how it does

so. Surveillance can be mobilised towards all kinds of governmental ends. Most extant democratic nation-states will tend to be found in this category or in that of Synoptic Democracy; Canada would be a primary example here.

High information flow produces the *Panoptic Polyarchy.* These are maximum surveillance societies. They have some democratic features but citizens are quite limited in their ability to access them. Information is collected to control and little is made available. The law supports the power of the state. Norris and Armstrong (1999)[5] argued that the UK was moving in such a trajectory.

Three questions then arise, which concern first, the extent to which surveillance practices can become accountable and transparent to stakeholders, including the public; second the extent to which they can be co-determined or at least negotiated; and third, whether public accountability is on the wane or on the increase –- in other words -- if there is a notable chilling effect in society. Because of the unequal power distribution between stakeholders, there are differences in who can demand transparency, i.e. who has access to the right resources and networks to render a surveillance practice transparent and accountable to their satisfaction. And there are of course dynamics in whether or not the watched can ever negotiate the terms of surveillance practices with watchers.

II.1 Aims and Objectives

The ultimate aim of the case studies was to identify the ways in which democratic processes can be made more resilient in the face of intensifying and pervasive surveillance. In relation to the empirical material this was operationalised by converging on the general question of how and whether democratic activities significantly featured within selected cases of surveillance practice, both from the perspectives of the watcher and the watched, and whether they mitigated its harms.

[5] Norris, C and Armstrong, G (1999) The Maximum Surveillance Society London: Berg

The empirical work was arranged around a broad structure of paired case studies of surveillance practices across Europe. In designing the cases it was decided that it was critical to capture the perspectives of both watcher and watched in relation to specified surveillance practices. Thus, the empirical work featured case studies of state-citizen surveillance from the perspective of both parties; private sector-consumer surveillance from the perspective of both parties and a stand-alone case study of citizen-citizen surveillance practices. Drawing on the DOW it was decided that three surveillance practices would be selected for paired case studies across the countries of those participating in the work package. It was felt that the following practices were sufficiently universal to be practiced across all participating states and sufficiently locally embedded to produce meaningful differences so we might understand how the practice became differentially embedded throughout Europe:

- State-Citizen/Citizen-State: Use of Automatic Number Plate Recognition cameras and databases by law enforcement agencies. Partners were: COMENIUS (Slovakia);USFD (UK) and UEdin (UK); Fraunhofer (Germany) VUB (Belgium)
- Private sector-Citizen/Citizen-private sector: Credit Scoring by Financial Services Institutions. Partners were UCSC (Italy); ITA (Austria); OU (UK); PRIO (Norway); Ekint (Hungary)
- Citizen – Citizen: Neighbourhood watch programmes. Partners were UH (Germany) and UniBW (Germany); STIR (UK); IRKS (Austria); UB (Spain)

A number of research objectives were set for the partners, as follows:

- Partners were to conduct mixed method case studies within a 12 month time period.
- The case studies were to focus on the perspectives of the watcher and the watched in order to get a top down and bottom up view of the practice.
- Partners were to obtain appropriate ethical approval where necessary
- After 12 months the partners were to produce a 5,000 word report detailing their responses to the research questions

II.2 Methods

In conducting their case studies, partners were encouraged to use secondary sources as much as possible to minimise the risks associated with gaining access to difficult sources. Key informant interviews were only used when absolutely necessary. Secondary sources included:

- Mainstream media reports and their analysis
- Policy documents and reports in associated trade press
- Corporate reports
- Freedom of Information Requests
- Academic sources
- Blogs and other online sources

Key informants were drawn from:

- Relevant law enforcement agencies, corporations or government
- Trade bodies or trade associations
- Trade unions
- NGOs
- Community organizations
- Journalists with a special interest in the practice
- Willing surveilled subjects.

In collecting their data, the partners were encouraged to consider a number of research questions. From the watched perspective, research focused on the questions detailed in box II.1, below, and from the watched perspective, the questions are outlined in box II.2 below.

The case study framework enabled partners to deploy a combination of data collection techniques which were appropriate to the national setting of the research. Tables detailing

those approaches are found in Appendix 1. Some key differences between each configuration of data collection are noteworthy:

1. Is information about the extent, nature and effectiveness of the surveillance practices:
   - accessible to the general public, specifically data subjects, and if so by what means
   - kept from the public, and if so, for what reason
   - publicly accountable to ethically and legally defined standards of conduct
   - open for discussion, debate and subject to co-determination, and if so, who is involved and how?
2. Have democratic interventions in surveillance processes increased or decreased over time?
3. Do watchers have any concerns, fears or vulnerabilities surrounding the effective operation of the surveillance practice; and have those concerns been allayed or intensified?
4. How have watchers have engaged with policymakers and regulators over the shape and form of the surveillance practice. If so, what happened and what was the outcome?

Box II.1 'Watcher' research questions

1. What is the watched's level of background knowledge about the respective surveillance practice: How has the practice been implemented, developed and used, and by whom?
2. What is the level of concern, fear or vulnerability about the surveillance practice?
3. Has that concern, fear or vulnerability been allayed or intensified?
4. Have the watched engaged with debates about any controversies which surround the surveillance practice?
5. Have they campaigned against the practice?
6. Have they changed in their behaviour around information collection and use, and if so, why?
7. Have they ever attempted to find out about their data double using subject access or FOI requests?
8. If they haven't, what their reasons were for not doing so?
9. If they did, what were their experiences?

Box II.2 'Watched' research questions

In ANPR, as an element of policy, a wider range of policy documentation was available, both from data protection and police authorities. Coverage in the legal literatures and also the mass media was significantly higher than in the other cases. In Credit Scoring, access to key informants within the credit scoring sector was very difficult to achieve, although informants who were customers were more forthcoming. In Neighbourhood Watch, only the UK case, which is very well established had a strong scholarly and policy literature base to analyse. In other countries analysis is based on media reports, social media, key informant interview and observational techniques.

Ethical approval was sought via institutional mechanisms where required. The entire design of the work packaged was discussed, evaluated and approved by the project's ethics board.

II.3 Analytical Framework

The case studies were initially conceived in terms of the analytical framework outlined in Work Package Two. Relations between the watcher and the watched were conceptualised as being shaped by a number of social, political and legal factors. It was thought that these factors would differ between European countries and an examination of these factors would reveal much about the dynamic interaction between surveillance and democracy across Europe. Figure I.1 summarises how we conceptualised the cases.

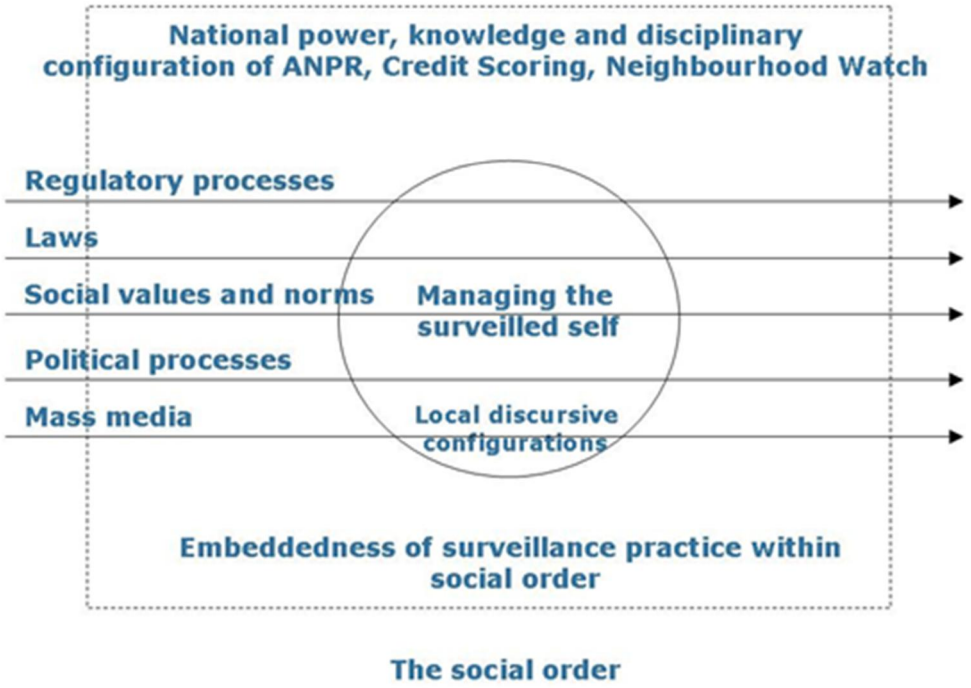


Figure II.1: Conceptualisation of the Case Studies in relation to WP2 framework

We were concerned how individuals managed their data flows, as watched, within the local circumstances of their lives. In turn, we conceptualised these individual experiences within national institutional frameworks which perpetuated, regulated and shaped the surveillance practice in question. In turn, these institutional frameworks were themselves shaped by broader, macro factors concerning regulatory processes, laws, social norms, political processes and the actions of the mass media.

In particular we were concerned to break down and operationalise the notion of democracy into three sub categories, or analytical levels, based on the factors identified in WP2. These three analytical levels were:

- *Governance*: The manner in which the surveillance practice is regulated and the extent to which different parties comply with regulation
- *Participation*: The extent to which the surveillance practice and its outcomes are co-determined by watcher and watched
- *Engagement*: The depth of personal interaction with the surveillance practice and the centrality of that interaction to the strategies of organizations and governments

Whilst a key aim of this deliverable is to chart the way in which democratic practices intersect with surveillance practices, a further objective is to chart the harms which arise as a result of surveillance practices. The nature of the harms which arise as a result of surveillance hence merits brief consideration. In 2006 Surveillance Studies Network (SSN) produced 'A Report on the Surveillance Society'[6] and outlined the specific characteristics of surveillance practices which may generate social harms, as follows:

Social sorting: Digital surveillance practices, such as ANPR or Credit Scoring, depend on the gathering and processing of personal data. As computer algorithms sort through the data, the population, as it appears in a database, is categorised in terms of risk. This categorisation process affords opportunities for some and disadvantages for others. Thus, there is a distributive justice element to social sorting.

Unintentional control: the intention of surveillance is often to manage, in an efficient way, flows of goods, information and people. However one person's management may be another person's social control. Surveillance signifies different things to different social groups, which may create perceptions of harm.

Information sharing: the efficient management of goods, information and people will require, in a surveillance society, information to be shared across all kinds of organizational boundaries. These requirements can leave both public and private sector organizations confused as to whether data protection regulations and apply, and how to apply them. As is

[6] Murakami Wood, D et al (2006) A Report on the Surveillance Society Wilmslow: Information Commissioners Office. http://www.surveillance-studies.net/?page_id=4 accessed 27th May 2014

the case with unintentional control, the desire to get things done may result in data protection and privacy being overlooked.

Blurring of the public and private: SSN notes that 'Whilst both public sector and private sector share information, boundaries between state and private sector interests are blurring, as more tasks of government are carried out through a sometimes complex combination of public, private, voluntary-sector and market mechanisms.'[7] The complexity of these organizational arrangements, once again, exacerbate problems of data protection as well as blur the locus of governance and regulation.

SSN then identify several harms which result from these characteristics of surveillance:

Anonymity and Privacy: because of the ubiquity of surveillance systems and the presence of unique identifiers about our person, either via our phones, vehicles, ATM and credit cards or TCP/IP addresses, it is increasingly difficult to achieve anonymity. Thus, one of the first pillars of privacy, anonymity, is compromised by surveillance practices.

Choice and consent: While the issue of consent arises straight away in relation to data processing surrounding information from various unique identifiers, there is little opportunity to opt out of surveillance.

Discrimination: speed, access and social inclusion. As social sorting delimits choices and sets category boundaries which ascribe advantages and disadvantages to social groups. The result of the is social sorting process is enhanced access and convenience for some, and increased barriers for others.

Democracy, accountability and transparency: In a telling paragraph, Ball and Murakami Wood (2006) outline how the three level of democracy drawn upon in this report – governance, participation and engagement – interweave in a surveillance society and leave citizens feeling ill equipped to challenge or question surveillance practices:

[7] Ball, K and Murakami Wood, D (2006) Summary Report: A Report on the Surveillance Society. Wilmslow: Information Commissioners' office http://www.surveillance-studies.net/?page_id=4 accessed 27th May 2014

Intensified dataveillance is becoming a normal feature in the modern state, and may, in itself, be justifiable – and justified by those who promote them – in the public interest. These activities may often be explicitly empowered by parliament. What makes them problematic is their manipulation of large quantities of personal data in ways that may overstep the mark established by data protection principles and laws, and by other constraints and guidelines about how information is to be collected, collated and communicated. We may become accustomed to being surveilled, our activities and movements tracked and also anticipated, without noticing it, and – especially in the public services – without the ability to opt in or opt out, or to understand fully what happens to our data. We may well accept as 'reasonable' the limitations on privacy that we might otherwise reject if we were to consider what being a citizen should mean. It is far from certain that the political situation will, at the end of the day, allow privacy rights to stand up strongly to the claims of government organisations made in the 'public interest', even if the public interest seems clear and of greater importance. If surveillance is meant to be 'proportionate', a lot depends on how that terms is interpreted, and on who interprets it. A lot also depends on the safeguards that surround the new, intrusive developments.[8]

As such four analytical notions of resilience are constructed in the face of the surveillance society and deployed in this deliverable. These four notions were derived from the position that surveillance is deployed to counteract harm, threat and risk, but that it simultaneously has harmful, risky or threatening consequences.

- Surveillance as a strategy to counter risk produces two types of resilience:
    1. *Resilience to and reduction of harm through increased safety and security:* When surveillance counters risk or threat in an effective way, increased safety, security

[8] Ball, K and Murakami Wood, D (2006) Summary Report: A Report on the Surveillance Society. Wilmslow: Information Commissioners' office http://www.surveillance-studies.net/?page_id=4 accessed 27th May 2014, page 15

and economic prosperity are experienced. The means of surveillance renders society more resilient to security, safety and economic threats.

2. *Resilience to surveillance by understanding its benefits:* If surveillance is commonly understood as an effective means of counteracting threat, then it becomes normalised and accepted more readily. Its harms are perhaps more readily accepted and are seen as being outweighed by its benefits.

- Surveillance as producing risks, threats and harms:
  3. *Resilience through the chilling effect:* When surveillance produces harm, chilling effects have also been observed as rights are denied and civic engagement declines. The chilling effect represents a homogenisation and/or stagnation of social, economic and democratic processes, as society puts its 'head in the sand', preferring to ignore what is going on. It is a very unproductive type of resilience to surveillance.

  4. *Resilience through increased awareness of surveillance and privacy and the development of critique:* If different sections of society engage with the harms produced by surveillance, resilience to its harms emerges in critical discourse against such surveillance practices and increased resistance to them. This also includes the discourse on consumer protection, data protection and constitutional law.

The problematic intersection between surveillance and democracy arises when surveillance becomes *the means to get things done*. Surveillance is an organizing process (Lyon, Haggerty and Ball 2012) the emergence of which was co-terminous with that of the modern bureaucracy. Surveillance embodies many of the desirable aspects of organizing: upward and downward information flow, feedback loops, and it can create transparency and accountability by making the actions of individuals and organizations more visible. However

to possess surveillance capacity is to possess power and the form of surveillance society which emerges depends on how that power is wielded and the extent to which it is scrutinised and open to critique. In the post 9/11 world, as surveillance became the means by which *security* was done and security practices became simultaneously exceptional and diffused into everyday life, the limits of democracy became apparent. As suspicion is now to be found, traced and pre-empted in everyday acts what then happens to everyday democratic practices and active citizenship? Furthermore with the blurring of public and private in the provision of security, the public accountability of security practices is more difficult to ascertain. According to Huysmans (2014)[9] democracy became 'at stake' as security policies threatened to hollow out human rights, compromise privacy and outflank rights to question, challenge and scrutinise. As surveillance and security are re-organized transparency and accountability need to do the same. Therefore democracy itself is a stakeholder in surveillance and security practices.

To interrogate the case study reports we have utilised the questions raised in WP2 relating to social, political and legal factors which surround surveillance practices, shown in table I.3, overleaf. The reports were treated as 'raw data' and were coded in NVivo. A total of 36 codes were produced which categorised the data according to the questions depicted in table I.3. The analysis which follows examines the answers to these questions and discusses the harms which arise as a result of these surveillance practices, then examines how they intersect with different levels of democratic practice. Finally it assesses whether democratic interventions can and should be strengthened in relation to the respective surveillance practices.

[9] Huysmans, J (2014) Security Unbound: Enacting Democratic Limits London: Routledge

Engaging (drawn from social questions):
How are the case surveillance practices perceived and understood by persons and by institutions? How is the surveillance practice depicted in the media? How have personal practices and corporate/governmental strategies been transformed by the surveillance practice, if at all? Do watchers and watched have any fears regarding the surveillance practice and has that fear been mitigated or intensified?
Participating (drawn from political questions):
Who is marginalised and whose interests are served by the practice? To what extent can surveillance data be accessed by data subjects? What other influences do data subjects have? How is the surveillance practice questioned or challenged, by whom and with what result? To whom are the watchers accountable, and with what result?
Governing (drawn from legal questions):
How is the practice regulated, and how does this differ between European countries? How effective are data protection laws in relation to the practice? Are they even relevant? What case law exists in relation to the practice and what does it say?

Table II. 1 Analytical questions

I.4 Report Structure

The report is structured as follows. Each of the surveillance practices are considered in turn: ANPR is followed by Credit Scoring and then by Neighbourhood Watch. Each surveillance practice is described and the stakeholders involved in each are outlined. Then, the harms which arise in relation to each practice are discussed. We then describe how democratic practices of engagement, participation and governance intersect with these practices to limit their harms. Each section finishes with a discussion of how the democratic processes may be made more resilient and key factors shaping international differences in the cases are identified.

CHAPTER TWO

AUTOMATIC NUMBER PLATE RECOGNITION

II.1 ANPR: An introduction to the practice

Automatic Number Plate Recognition, or ANPR, is a surveillance practice in which digital CCTV cameras capture images of vehicle registration plates. These images are then matched to government vehicle licensing and other databases which contain information pertaining to the ownership of the vehicle, whether it is insured or whether it has been marked as suspicious in any police investigation. Once the data have been cross-checked against these databases – a process that takes around 1.5 seconds to complete – information about the vehicle, its registered owner and driver appears on a computer where it is assessed by ANPR-trained police officers. If the information supplied via the ANPR system alerts officers to an offence or relevant intelligence on a vehicle, the vehicle will be stopped to allow officers to investigate further. ANPR is also used to administer car parking and road toll charges. Users of ANPR are thus not only public bodies such as the police, city and regional municipalities and national government agencies, but also private companies who compare images from the cameras with their own customer databases. Fixed or mobile cameras can be used as part of an ANPR system and it can be deployed in an overt or covert way, depending on the legal regulation under which it is deployed.

In this case study ANPR in four European countries was examined. Uses and intended uses are remarkably similar across the countries. It is clear that some countries are in a more advanced state of ANPR use (for example, the UK) whereas in others it is emergent (for example, Slovakia):

Belgium: Here, ANPR is used to detect traffic offences (such as whether the driver is disqualified or uninsured) and to ensure road safety by detecting vehicle speeds. It is

increasingly being used as a tool to combat crime more generally comparing number plates against police databases which indicate whether a vehicle has, or is suspected of being used in a crime. Nationally registered vehicle plates are matched against the directory of Belgian car number plates (within the Federal General Directorate for Mobility and Road Safety), whereas the Schengen Information System (SIS) is used to identify vehicles from other European countries.

Germany: In Germany, ANPR is applied in four ways: first, to support the police in their crime prevention and law enforcement activities; second, to administer road tolls for truck drivers; third, as part of private security systems for building access and fourth, for traffic management, e.g. to count the number of cars moving on a specific street. In principle it is possible to match ANPR images against a number of databases similar to those used in Belgium, but in practice this differs between the *Länder* and is dependent on the specific regulations of their respective police laws. Brandenburg for instance compiles a specific data file for each case. In contrast, Bavaria uses existing databases such as INPOL and SIS. As such, each of the 16 *Länder* has its own history of ANPR. Some have never used ANPR, some have stopped using it and some still use it. Currently, 11 *Länder* have specific regulations covering ANPR. Nevertheless, not every *Land* that adopted particular provisions for ANPR, applies those provisions. In turn, other *Länder* both have provisions that are of questionable constitutionality and apply them.

Slovakia: ANPR is an emergent surveillance practice in Slovakia. It is deployed, or is to be deployed in several areas. In terms of its proposed uses, first, it is going to be used to control vehicle access in buildings and car parks. It is also going to be deployed alongside two new databases (Central Registry For Offences and National System of Traffic Information, planned for 2015) that will use ANPR data for monitoring and for law enforcement. Third, it will be installed in police cars as a part of a new hardware project that was launched in 2013 and will be implemented from 2014 onwards. Fourth, it is currently

being tested as a means of enforcing legal changes which will instantiate ‘no fault’ driving offences. Finally, and the only area in which it is fully implemented, is in the Electronic Toll System (ETS), which administers road tolls, launched in 2010.

United Kingdom: ANPR is used very extensively in the United Kingdom. Police and local authorities are the dominant users of ANPR. ANPR systems are able to check up to 3,000 number plates per hour, per lane, even at speeds of up to 100 mph on a motorway. These reads are initially processed locally at each police force's Back Office Facility (BOF), and then they are transferred to the central National ANPR Data Centre (NADC) which ”stores all number plate reads collected by local forces making them available for researching nationally”. The NADC can provide information on vehicle movements that can assist the police in identifying patterns of behaviour of targeted individuals. By 2012 it was reported that the National ANPR Data Centre was receiving more than 18 million number plate ‘reads’ each day and that the database holds details of 11.2 billion vehicle reads. As well as vehicle tracking and identification, a unique use of ANPR in the UK is to generate intelligence profiles of suspects as an aid to criminal investigation. It is now possible for UK police forces to interrogate in excess of 7 billion records per year lodged on the system. The main ways that the data can be exploited through data mining are outlined as:

- vehicle tracking: real time and retrospective;
- vehicle matching: identifying all vehicles that have taken a particular route during a particular time frame;
- geographical matching: identifying all vehicles present in a particular place at a particular time;
- incident analysis: can be used to refute or verify alibi statements, to locate offenders, to identify potential witnesses to specific incidents by identifying vehicles in the location at the time of an incident;
- network analysis: by identifying the drivers of vehicles and their network of associates, ANPR can be used to indicate vehicles that may be travelling in convoy;

- subject profile analysis; by creating an in depth profile of the suspects by integrating information from a variety of data sources such as "crime reports, incidents reports, witness testimony, CCTV, other surveillance, communications analysis, financial analysis, as well as existing intelligence, to define a pattern of behaviour for a subject of interest".

Private companies use it to monitor vehicular access to public and private sites and their associated car parking spaces. It is increasingly used to monitor and enforce payment for car parking, in a range of public and private schemes. Here the scheme operators can gain access to the Driver and Vehicle Licensing Agency's (DVLA) database of registered keepers, 'with the reasonable cause of broken contract for parking on private land'. It is also being increasingly used by local authorities to enforce bus lane restrictions and other infringements of traffic laws, such as the congestion charge in London.

Reviewing the uses of ANPR across Europe, it is clear that it is deployed to counteract certain harms: crime both in terms of driving offences and broader criminal offences, terrorism, road toll evasion, as well as to promote road safety and to manage traffic congestion and flow.

II.2 Stakeholders in ANPR

Figure II.1 below illustrates the stakeholders involved in ANPR. We draw upon the business definition of 'stakeholder' as an entity who is influencing or influenced by something, in this case, the practice of ANPR (Freeman 1983).[10] Stakeholders are divided into two groups: core stakeholders, the 'watcher' and 'watched' as we defined the original case study format and peripheral stakeholders. Peripheral stakeholders are those who are not directly involved in watching or in being watched but who have engaged with the practice either through regulation, other policy areas such as economic and regional development, activism,

[10] Freeman, R. E. (1983). Strategic management: A stakeholder approach. *Advances in strategic management*, *1*(1), 31-60.

finance, infrastructure or systems provision, or interest group representation such as drivers associations. The stakeholders represented in the diagram are an amalgamation of information provided from across the four cases. In the diagram the influence of peripheral stakeholders is conceptualised in relation to the 'watcher-watched' nexus rather than either on the side of the watcher or the watched. This may be the case, however, in relation to some stakeholders, such as human rights organizations who campaign against ANPR on privacy and other human rights grounds. Implicit within a stakeholder analysis is the notion that different stakeholders will exert different degrees of influence over the practice and legitimacy in respect of it. These differences emerge when we consider the harms arising from the practice in the next section.

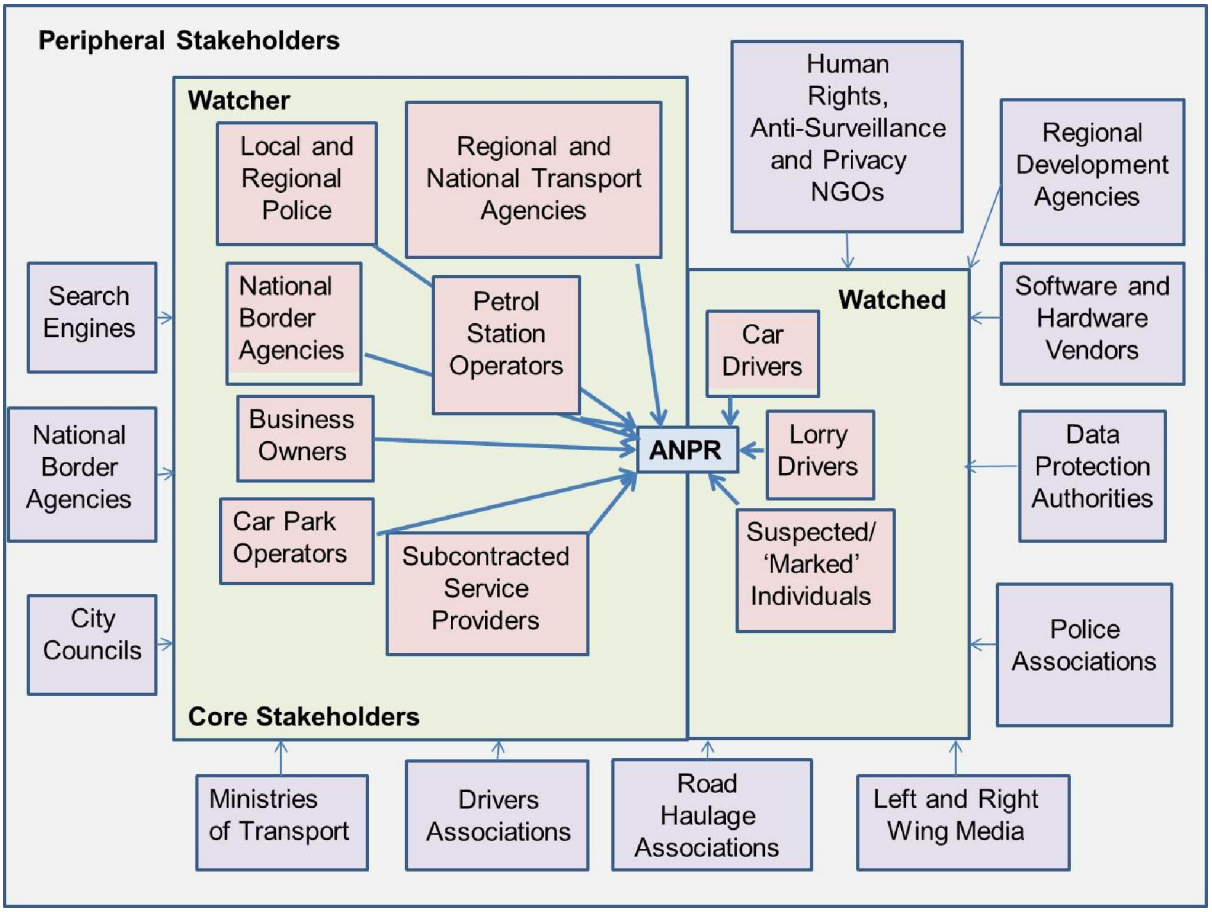


Figure II.1: Core and Peripheral Stakeholders, ANPR

II.3 Harms and controversies arising from ANPR

The harms and controversies which arise from ANPR begin to highlight where democratic resilience needs to be strengthened in the face of it. All but one of the harms we examine here are 'stresses' rather than 'shocks' in that they are issues which persist at a low level and are highlighted from time to time. We consider the stresses first and then move on to the one shock in the UK which curtailed more intensive use of ANPR.

II.3.1 Stresses

In this section we examine the ways in which ANPR has caused stresses around democratic matters. There are a number of examples concerning the operation of the rule of law, the presumption of innocence, freedom of movement, privacy, transparency, economic and environmental harms.

II.3.1.1 The rule of law, freedom of movement and the presumption of innocence

Instances from Belgium, Germany, Slovakia and the UK highlight how the implementation of ANPR has compromised the rule of law, exploiting loopholes as technology development and deployment outpaces regulatory developments. NGOs such as the Flemish League of Human Rights (FLHR, Belgium) are keen to point out these instances. In *Belgium*, for example, the use of mobile ANPR does not have a basis in law and as such no limitations about the use of this technology have been established. FLHR are also keen to point out that because ANPR automatically captures drivers' details it bypasses the presumption of innocence as well as compromising freedom of movement.

The issue of legal limitation also arose in *Germany*. The Federal Constitutional Court's decision concerning ANPR in 2008 has heavily shaped the use of ANPR in Germany. Discussions about the legality of ANPR were initiated in Hesse. In 2005, a new police law was introduced that allowed the Hesse police to use it without a specific reason and without restriction to a specific street. Following this, the Hesse Constitutional Court received a

complaint about ANPR in 2008. In this statement the plaintiff referred to the 2006 decision of the Federal Constitutional Court on dragnet investigations (a dragnet investigation occurs when everyone in an area is stopped and searched if a criminal is shown to be in a particular area). The Court had ruled that dragnet investigations were only allowed if a concrete danger existed – a general situation of increased threat is not sufficient for an encroachment on the fundamental right of informational self-determination in Germany. In 2008 the Federal Constitutional Court decided in 2008 that the challenged provisions in Hesse and Schleswig-Holstein were unconstitutional, ruling:

> "The provisions do not comply with the precept of determinedness and clarity of legal provisions because they neither determine the cause nor the purpose of investigation which both the recognition and the matching of the data are intended to serve. Over and above this, the challenged provisions, in their undefined scope, also do not comply with the constitutional precept of proportionality. They make severe interference with the affected parties' right to informational self-determination possible without sufficiently codifying the statutory thresholds which fundamental rights demand for measures that constitute such intense interference." [11]

The Court argued that the fundamental right to informational self-determination had been infringed, if the number plates "are not promptly matched against the tracing files and deleted without further evaluation".[12] Furthermore, the challenged provisions did not fulfil the requirement that "interference with the fundamental right to informational self-determination must have a statutory basis that is constitutional".

Legal problems arose in *Slovakia* pertaining to potentially corrupt tendering procedures for ANPR service contracts. During the preparation phase of ETS several political

[11] Kenzel, Brigitte, *Die automatische Kennzeichenfahndung. Eine neue Überwachungsmaßnahme an der Schnittstelle zwischen präventivem und repressivem Einsatz*, Verlag Dr. Kovaĉ, Hamburg, 2013.
[12] Ibid

commentators pointed out the size and scale of the project (the estimated value of the contract was believed to be around 660 million EURO) and its "attractiveness" for interest groups close to political parties in the government. When the contract was awarded, it emerged that the National Highway Company (NDS) that procured the system on behalf of the state excluded three out of four bids for failing to meet technical requirements. The one company which remained was the most expensive bid (at 852,1 million EURO). The procurement is still subject of an ongoing infringement procedure initiated by the European Commission "for breaching European legislation by failing to announce a Europe-wide tender for its electronic road-toll system operator and discriminating against candidates in the tender process".[13] Despite the legal challenge from the EC, and several legal challenges from companies that submitted failed bids, the winning consortium SanToll - Ibertax signed a 14 year contract (with five year option) in January 2009.

In the *UK*, in 2011, three privacy rights groups, 'Big Brother Watch', 'No CCTV' and 'Privacy International', used the rule of law to challenge ANPR. They made a formal complaint to the Information Commissioner that the ANPR surveillance around the town of Royston was operating unlawfully. Royston is a small town in Hertfordshire, with a population of 15,000 people, which sits on a convergence of east and west routes between the major national roads of the A11, the M11 and the A1M. Hertfordshire Constabulary as part of the National ANPR network had installed 7 cameras on all the approach roads in and out of the town, which effectively meant that "no vehicle could enter or leave Royston without being recorded on camera".

The complaint about the Royston system raised a number of issues, the principle of which was that it was extraordinary that such an extensive surveillance network could be constructed "without the result of any Parliamentary debate, Act of Parliament or even a Statutory Instrument". Furthermore they complained that the national ANPR strategy was

[13] See European Commission, Public procurement: Commission calls on Slovakia to respect EU rules for electronic toll collection contracts, 30/09/2010, Available at: http://europa.eu/rapid/press-release_IP-10-1244_en.htm?locale=en, accessed 08/11/2013

run by a police association called ‘The Association of Chief Police Officers’ which was not accountable to parliament. More examples from this complaint will be cited in later sections of the report.

Beyond the specifics of the Royston case, closer examination of the laws surrounding ANPR use in the United Kingdom reveal that there is no specific law which governs or sanctions it. This was confirmed by the ACPO's rather terse response to a recent Freedom of Information (FOI) request which stated:

> The use of ANPR merely provides information on which officers may act. It does not require any legislation or statutory powers. [14]

As with general open street CCTV, there is no law that expressly gives them this right to record and store images and information derived from them. However, because a car number-plate, like a picture of a person, may be considered personal data, the data is subject to the provision of the Data Protection Act. And although the Act does expressly give them the right to store ANPR data, it does limit the length of time that it can be retained and creates the legal basis upon which information can be processed and shared. This is why the NGOs challenge to the use of ANPR in Royston was framed in terms of data protection legislation.

However, where a camera is covert and the purpose of its operation is to target specific individuals, then it constitutes 'directed surveillance’ under the provision of the Regulation of Investigatory Powers Act 2000 (RIPA). This requires high level and special authorisation and reporting to the Office of Surveillance Commissioner, whose job it is to oversee covert surveillance. As various FOI requests have found, for operational reasons, the police are not prepared to identify the sites of ANPR operation, neither do they generally warn motorists that an area is under ANPR Surveillance and some cameras are, indeed, really 'covert'. Given that the positioning of ANPR cameras is deemed secret, then the issue

[14] Details of statutory powers relating to ANPR made by Marie Koenigsberger under the Freedom of Information request to ACPO on the 4th September 2009. Avialable at: https://www.whatdotheyknow.com/request/details_of_statutory_powers_rela?unfold=1

arises as to whether they constitute a covert surveillance device. For covert surveillance to be legal it needs to have an express legal basis, but there is no statutory basis for the operation of ANPR, as widespread usage was not considered when the RIPA was introduced.

It would seem that the law that does, in some circumstances, regulate the use of ANPR, but this is being sidestepped by the police. They appear to be routinely using the ANPR database to carry out directed surveillance without RIPA authorization, so much so that the Surveillance Commissioner accused them of deliberately circumventing the law. This lack of attention to their legal obligations was also noted by the Thornton review of Project Champion, which concluded:

> There was, however, nothing available to the Review Team that demonstrated that the authorisation process for the use of the cameras had been considered, and there was no policy, plan, or procedures in place for their management in compliance with RIPA or other applicable legislation, codes, or guidance.[15]

II.3.1.2 Privacy

Numerous privacy issues arise in relation to ANPR. The main issue is notice – most drivers across Europe do not know the difference between an ANPR camera and a normal CCTV camera since they are not required to be labelled any differently. Moreover it is difficult to persuade police and other operators to disclose the location of ANPR cameras. In *Belgium*, for example, it is impossible to avoid ANPR-related checks when crossing the Belgian border. Similarly, drivers cannot divert their route only because there are ANPR devices in operation on a certain highway. Most of all, given the recent use of ANPR systems in Belgium, drivers do not know where and when they will be subject to mobile ANPR cameras.

[15] *Thornton, S. (2010)* Project Champion Review: An independent review of the commissioning, direction, control and oversight of Project Champion; including the information given to, and the involvement of, the community in this project from the initiation of the scheme up to 4 July 2010; Thames Valley Police.

Being against the principle of foreseeability (Art. 8.2 of the European Convention on Human Rights), the implementation of many ANPR schemes may well fail privacy impact assessment.

In *Slovakia* the ETS has been the subject of a political debate which questioned its implications for privacy. During the 2010 parliamentary election campaign, an opposition MP, S Janiš, organized a press conference which accused the ETS operator, SkyToll of mishandling the ETS databases. He was particularly critical of the fact that they had used unidentified overseas partners to provide information systems. A parliamentary enquiry also accused the CEO of SkyToll to have made inappropriate disclosures of toll customer account information pertaining to the head of the Truck Drivers Union, vociferous in their opposition of ETS. Despite significant media coverage, and even though the Slovak Ministry of Transport launched an investigation, the case vanished from media and was not followed legally or politically.

Returning to the British town of Royston, the substance of the complaint made by three NGOs related to its legality under the Data Protection Act. They alleged that the system breached the second principle of the DPA which states that "personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose" [16] Their objection rested on the basis that the justification put forward by Hertfordshire Constabulary was:

> "vague at best and furthermore it seems that Hertfordshire Constabulary along with other forces believe that they can simply state objectives without any evidence that the objectives are attainable. This is an absurdity. The fact that the stated purposes

[16] Complaint by NO CCTV, Privacy International, and Big Brother Watch to the Information Commissioner, with regard to 'Royston ANPR Ring of Steel', the full text of the complaint is available at: http://www.no-cctv.org.uk/materials/docs/Royston_Ring_of_Steel_ANPR_Complaint.pdf, page 4

> of ANPR are not backed up by evidence that they are attainable must surely further undermine Hertfordshire Constabulary's compliance with principle two of the Act.[17]

They also argued that the system was in breach of the fifth principle of the DPA which states: “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes”.[18] The complainants argued that Hertfordshire Constabulary appeared to be keeping data for longer than the legally proscribed period of two years, and that even this retention period was excessive.

A further complaint was that the first data protection principle that data should be processed fairly and lawfully requires that "part of fair processing is the requirement to notify people that they are being filmed".[19] The absence of signage in the Royston system makes it in breach of the fair processing requirement. Finally, the complained that under the DPA, for data processing to be lawful, it must be ‘necessary’ and ‘proportionate’ and that such an extensive blanket surveillance is neither. As they argue:

> In the past totalitarian regimes instituted road blocks to check citizens' papers at a series of internal borders. The police use of ANPR as a mass surveillance tool to record the movements of all cars and the justification given by Hertfordshire Constabulary for a ring of cameras around Royston such that “no vehicle could enter or leave Royston without being recorded by a camera” because the town is in “a location of importance on the borders of Hertfordshire and Cambridgeshire” is surely equivalent to an automated checkpoint system that cannot be necessary in a democratic society to meet any of the purposes set out by Hertfordshire Constabulary.[20]

[17] Ibid, page 7
[18] Ibid, page 9
[19] Ibid, page 10
[20] Ibid, page 12

It took the Information Commissioners' Office (ICO) two years and one month to rule on the complaint. On the 15th July 2013, the ICO issued an enforcement notice against the Chief Constable of Hertfordshire Constabulary requiring that the data controller:

> Refrain from processing personal data… except to the extent that such can be justified to the satisfaction of the Commissioner as being in compliance with the First and Third Data Protection Principles following the conduct of a Privacy Impact Assessment or similar impact assessment that defines the pressing social need, assesses the likely effectiveness of the proposed measures in addressing this, identifies the likely impact on the private life of individuals and determines that the proposed measures are a proportionate interference after taking into account any additional safeguards that might be provided.[21]

Hertfordshire Constabulary duly conducted a Privacy Impact Assessment and removed an unspecified number of cameras. Subsequently, the ICO declared itself to be happy as to the proportionality of the scheme. The ruling did not satisfy the complainants. In their view it represented a hollow victory because the ICO had "side stepped" the real issue by reducing the complaint to a balancing of the ECHR article 8 right to privacy against the State's right to qualify it for particular purposes. In effect the ruling merely asked the police to state the reasons for the qualification of the right, thereby reducing the "whole issue… to a meaningless box ticking exercise".[22]

II.3.1.3. The right to protest

In the UK, ANPR is being used to surveill the movements of those who have been lawfully engaging in their democratic right to protest. The surveillance of political activists and protesters has long been a function of the British police. In 1882 a 'special branch' was formed as part of the Metropolitan Police after a spate of Fenian bombings in London and,

[21] http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf. Page 3

[22] ICO ruling replaces "Ring of Steel" with Mass Surveillance Roulette - 7/3/14 - available at: http://www.no-cctv.org.uk/press.asp

while the surveillance of the Irish republican movement remained the central remit of Special Branch for almost the next hundred years, its mission was extended to include anarchists, communists, peace campaigners and trade unionists, to name but a few.

The most recent incarnation of the surveillance of activists and protesters has been carried out by the National Domestic Extremist Unit, which was directed by the Associaiton of Chief Police Officers (ACPO) Sub-Committee on Terrorism and Allied Matters. In the wake of a number of scandals, in 2011, the management of domestic extremism units was moved from ACPO to the Counter Terrorism Unit of the Metropolitan police, which is now responsible for the National Public Order Intelligence Unit (NPOIU). NPOIU runs the database of 'domestic extremists' which collates intelligence supplied by police forces across England and Wales and deploys its own surveillance teams at demonstrations and sites of political protests.

The ACPO definition of domestic extremism is as follows:

> "Domestic extremism and extremists are the terms used for activity, individuals or campaign groups that carry out criminal acts of direct action in furtherance of what is typically a single issue campaign. They usually seek to prevent something from happening or to change legislation or domestic policy, but attempt to do so outside of the normal democratic process.[23]

The operational enactment of this concept has been criticised in a recent Her Majesty's Inspectorate of Constabulary review as being far too wide ranging. In particular there have been allegations that almost anyone attending a political protest may be subject to intimidating surveillance tactics which include "following, stop and searching and, photographing peaceful protestors by Forward Intelligence Teams (FITs)".[24] In June 2013, it

[23] The ACPO definition is cited at page 11 of http://www.hmic.gov.uk/media/review-of-national-police-units-which-provide-intelligence-on-criminality-associated-with-protest-20120202.pdf
[24] The Guardian Newspaper "Are you a 'Domestic Extremist'?

was reported that 8,931 individuals had a record on the Domestic Extremist database and that, “Senior officers familiar with the workings of the unit have indicated to the Guardian that many of the campaigners listed on the database have no criminal record.”

While the activities of the Police FITs has come under scrutiny, it is clear, however, that ANPR data is being used to routinely track and monitor political protestors and then to log them on the 'domestic extremists' database, and that inclusion on the database is not confined to those who perpetrate violence and disorder. Merely being "associated" with protests that have given rise to "crime, disorder and the deployment of significant resources",[25] appears to give the police sufficient justification to include a person on the database and subject them to extensive tracking and repeated stops. But even those attending peaceful protests have also been logged. As the Guardian newspaper revealed, a man with: “no criminal record, was stopped more than 25 times in less than three years after a 'protest' marker was placed against his car after he attended a small protest against duck and pheasant shooting”.[26] Similarly, John Catt, an eighty-five year old peace campaigner and his fifty year old daughter had their presence recorded at over 80 lawful demonstrations over a period of four years. As well as information gained by Forward Intelligence Teams, Mr. Catt's movements were also being recorded on the emergent National ANPR Network. In July 2005, he and his daughter:

> were stopped by police under the Terrorism Act after driving into east London to help a family member move house. They later discovered police had placed a marker against their car registration on the database, triggering an alert – "of interest to public order unit, Sussex police" – each time they drove beneath an automatic number plate reading camera.[27]

[25] http://www.guardian.co.uk/uk/2009/oct/25/surveillance-police-number-plate-recognition
[26] http://www.guardian.co.uk/uk/2009/oct/25/police-domestic-extremists-database
[27] http://www.theguardian.com/uk/2010/jun/25/peace-campaigner-classified-domestic-extremist

In 2009, Fitwatch (which is an NGO devoted to reporting on the activities of 'Forward Intelligence Teams') reported that ANPR units were being used to monitor and intercept climate change activists' cars during the protests around the Kingsnorth Power station. However much of the police activity was declared unlawful when three activists were awarded compensation from the Kent Police who admitted "they had been unlawfully stopped and searched".

II.3.1.4 Transparency

The more widespread and sophisticated use of ANPR in the *UK* has prompted greater public awareness of the practice as well as attracting the attention of the media, privacy and human rights campaigners. In July 2009 the Guardian Newspaper filed a FOI request on behalf of the Guardian asking for the locations of the ANPR cameras used by the Devon and Cornwall Police. The Devon and Cornwall Police refused, relying on exceptions under the FOI (2000) in relation to the prevention, detection, and prosecution of offenders, the administration of justice and national security. On appeal, the ICO said that Devon and Cornwall Police were correct in refusing to provide the locations of automatic number-plate recognition cameras although it accepted that the extent of the ANPR network "is of considerable significance to the balance of the public interest".[28] The Guardian then took their complaint to the Information Rights Tribunal, who set aside the ICO decision, instead ruling that the effectiveness of ANPR in fighting crime was not altogether clear. On balance, they ruled it was in the public interest to disclose the location of the cameras so that people could exercise their rights under the Data Protection Act if they so wished. However this was then overturned again, by a different panel of the Information Rights Tribunal, who argued that the national security exemptions under the FOI Act (2000) did apply.

[28] Reference: FS50270424,Freedom of Information Act 2000 (Section 50),Decision Notice, Reference: FS50270424, Date: 23 September 2010, page 7.Available at: http://ico.org.uk/~/media/documents/decisionnotices/2010/FS_50270424.ashx page 7.

Similarly the right of Information Self Determination in *Germany* has led to some legitimate legal challenges of police laws which sanction ANPR use. The Federal Commissioner for Data Protection and Freedom of Information and also some data protection commissioners of the *Länder* criticised the lack of transparency in the negotiations between the Federal Ministry of Transport, Building and Urban Development and the corporations responsible for the implementation of the ANPR system. However in Belgium public debate has only recently taken place and in Slovakia it is barely covered at all. In a manner similar to Germany, consultation processes in the Belgian implementation phases of newer ANPR systems have been criticised and the DPA was excluded altogether.

II.3.1.5 Economic harms

The introduction of ANPR in *Slovakia* is partly backed by regional development agencies keen on improving transport infrastructure and trade links with the rest of Europe. However the wide-ranging economic rationales for the introduction of ANPR has prompted a significant body of economic opposition to the initiative. The main body of opposition has come from the truck drivers and the professional association. The high cost of the ETS has prompted ever increasing toll charges, payable by the trucking companies and by individual drivers, which, they argue, threatens their economic livelihoods. It has also prompted them to use GPS jammers which disrupt the ETS signal and enable the toll to be avoided.

In March 2010, several weeks after the ETS became operational, the most popular Slovak weekly Plus 7 dni printed a report titled "Ďalší Škandál" (Another Scandal)[29] on alleged use of GPS jammers that allowed truck drivers to avoid the toll. It criticized the expensive control system that was, allegedly, unable to cope with cheap GPS jammers that were widely available in e-shops in UK, Poland and Czech Republic. The reporters successfully tested a jammer with anonymous transport company. The article also pointed to the fact that the

[29] See, Plus Sedem Dní, Ďalší škandál (Another Scandal), 26/10/2010, available at: http://www.pluska.sk/plus7dni/vsimli-sme-si/dalsi-skandal.html, accessed 03/11/2013

police did not have appropriate technical equipment to handle jammers. Various media outlets picked up the story. The Daily SME published several articles over the following weeks that asked for comments from Narodna Dialnicna Spolocnost (NDS), the Police and the SkyToll representatives. While NDS refused to comment, SME managed to interview the Chief of the Toll Police who said that he was not a person to comment and "that he never heard about the GPS jammers".[30] A popular online car section of SME also produced a nine-minute video segment on jammers that explained their use. A software engineer explained that the use of jammers was nothing new in Slovakia and that his company had to solve problems of drivers that were avoiding GPS surveillance by their bosses in transport companies by using jammers. The report avoided explicit reference to the ETS, and ended up with a statement by a press officer from Telecommunication Office of Slovakia, who stressed that any use of jammers was an offence punishable by a heavy fine, both in Slovakia and EU. A few weeks later SME published another article on the use of GPS jammers. The article cited an official from one of the interest groups who confirmed that he also has information [31] about use of the jammers and pointed to the fact that this is "unfair for all those who are paying dutifully". The newspaper also obtained, from anonymous source, a report about test on efficacy of the ETS, which concluded that out of 12 control gates only one was functioning and that the system was unable to deal with the GPS jammers. Both the NDS and the SkyToll refused to comment. In follow-up article next day, the SkyToll representative pointed out to the fact that jammers were illegal and that the company knew how to "handle invisible cars". The Toll Police refused to provide any data on the enforcement of the ban. This series of articles was last one that investigated use of jammers in the ETS.

[30] See SME, Mýto vraj kamióny obchádzajú rušičkami, (Toll Is Allegedly Avoided by the Use of Jammers) , 26/03/2010, http://ekonomika.sme.sk/clanok.asp?cl=5302262, accessed 09/12/2013
[31] See SME, Rušičky z mýtnych ciest nezmizli (Jammers Still on Toll Roads), 30/05/2010, available at: http://s.sme.sk/r-rss/5399308/ekonomika.sme.sk/rusicky-z-mytnych-ciest-nezmizli.html, accessed 09/10/2013

The Toll Police then changed their communication style informing the media about ETS enforcement at regular intervals: e.g., in 2012 the Toll Police, together with the Telecommunications Office of Slovakia performed 87 operations that found 26 jammers, same amount as in 2011. It is impossible to gather hard data on the scale of the use of the GPS jammers in the ETS. Media analysis provided only anecdotal evidence; the official data from police include dozens of cases for 2011 and 2012. Several comments under the theme "Bad Companies" on Profivodic.sk, a site for professional drivers, also identifies the companies where management forces drivers to avoid the toll by using jammers. While the GPS jammers still remain easily obtainable via the Internet, websites that sell them include a legal disclaimer about their ban and sole legal responsibility of the buyer.

In January 2013, the Truck Drivers' Union launched an information campaign and a petition demanding various changes in the ETS, a reduction in excise taxes on motor fuel and decreases in road tax rates. In the following weeks the Union organized several protests across Slovakia and in Bratislava, dozens of trucks blocked several main roads. All media reported the blockade and in the election year it caught the attention of both the government and the opposition. It ended after several rounds of negotiations between the government and various interest groups. The Prime Minister R. Fico announced that his government will accept some of the demands from haulers associations and business community (e.g. Chamber of Commerce), which included introduction of a ticketing system for several roads near state borders, lowering of excise taxes on motor oil and the temporary suspension of toll payments on 1st class roads. The Transport Minister Ľ. Vážny also survived a no-confidence vote in the parliament after the opposition demanded his resignation for troublesome implementation and launch of the ETS.

During the protests of transport companies the media reported that a tollgate was destroyed at a 1st class road near Bratislava. The Prime Minister R. Fico mentioned the incident during

his press briefing, saying, "This is a road to hell".[32] Mr. Fico warned everyone who is going to destroy tollgates to be prepared for consequences. Soon after another tollgate was destroyed and its hardware stolen but this was the last reported incident of direct protest action. Although the Union of Slovak Haulers remained on strike for rest of the year, unsuccessfully sued SkyToll for faults of the ETS in 2010 and threatened with another blockade in 2011, the new leadership of the Union changed their tactics and started to concentrate their efforts on more traditional lobbying activities to demand favourable conditions for hauliers in Slovakia. Hauliers associations were extensively consulted about the new law on toll introduced in 2013, in which the government compromised on a proposal to increase toll rates automatically with the inflation, which they groups refused. Negotiations are ongoing.

The *German* drivers association (ADAC) also positions itself against ANPR, commissioning and publishing a study which was strongly critical of the additional costs it imposed on drivers. ADAC represents 14 million German motorists and is a powerful lobbying group. Its actions, however, fell way short of the direct action and protest witnessed in Slovakia.

II.3.1.6 Environment and quality of life

Part of the rationale for ANPR-based road tolling, particularly in relation to heavy freight traffic, is to encourage haulage companies to maximise the load on their vehicles and reduce the number of journeys they make. This has the benefit of reducing congestion and fuel consumption, as well as encouraging firms to invest in more fuel-efficient vehicles. However this environmentally friendly rationale for tolling is counteracted – in the Slovakian context at least – by drivers avoiding tolls and driving heavy trucks along toll free roads which are inappropriate for vehicles of that size. This resulted in an increase of heavy vehicle traffic in smaller towns and villages, with excessive damage to property and the local road

[32] SME, Podpílili mýtnu bránu, zasahovala do cesty (Someone destroyed TollGate), 28/01/2010, available at: http://auto.sme.sk/c/5213337/podpilili-mytnu-branu-zasahovala-do-cesty.html, accessed 08/09/2013

infrastructure. A solution to this problem has yet to be found. Part of the issue is that the national government owns and controls the main roads, whereas regional governments control the local roads and so no appropriate and consistent policy instruments can deal with the problem. Furthermore Slovakia had three national governments in as many years from 2010 – 2013.

In August 2012, The Daily SME published, as a part of "Personalities Make Newspapers series",[33] a long report about the problem. Slovak singer and actress S. Tobias reported her personal experience in her village that was devastated by large trucks avoiding the toll. A video attached to the report showed the village of Lednice, where it took two and a half years to have no entry traffic signs installed by state authorities. “If we move to the front room, you will feel the ground shaking. It is worst on Sunday evening. We cannot sleep. It is depressing", said one of the villagers for the newspaper.[34] In the small village of Dvorianky, citizens organized an informal group that systematically monitored the situation. In order to provide precise data to state administration on traffic and types of vehicles that were using their road, they used infrared cameras. They have their own Youtube channel with video footage of trucks in various time periods, a blog, a webpage and a Facebook account. In 2013, after months of complaining to various level of the government, it was decided that the main road that ran through their village would be included in the ETS from January 2014. However, as a blog post of the petition chairman argues, the effectiveness of the signs remains to be seen, as the toll for using their road will be cheaper compared to a parallel highway.

In 2011, the Transport Ministry discussed the proposal of a nation-wide ban of heavy vehicles from local roads, but decided instead to increase the number of no entry signs in

[33] SME, Kamionisti šetria na mýte a ničia domy i život v obciach (Trcks save on toll and destroy properties and life in villages), 24/08/2012, available: http://www.sme.sk/c/6509458/kamionisti-setria-na-myte-a-nicia-domy-i-zivot-v-obciach.html, accessed 09/11/2013
[34] ibid

several problematic areas. After the 2012 parliamentary elections, the New Interior Minister R. Kaliňák acknowledged that there has to be a more coordinated effort to solve the problem that will also include legislative changes. The problem of avoiding the toll roads is addressed in the new 2013 law. The law extends ETS to roads of 2nd and 3rd class (with zero toll) and once again, significantly increases fines for use of these roads. The extension will allow for better monitoring of the traffic and increased enforcement that will cover more roads. The change in the new 2013 law confirmed that current enforcement was not able to handle the scope of this problem, despite repeated complaints from communities, regional politicians and media. Ironically, public engagement and campaigning around the ETS has led to a greater extension of surveillance.

II.3.2 Shocks

We now examine a specific controversy – or shock - surrounding the implementation of ANPR: Project Champion in Birmingham UK. In this example, ANPR became the unacceptable tool of ethnic targeting and discrimination.

II.3.2.1 Ethnic targeting and discrimination: The case of Project Champion

Project Champion was a scheme which encircled two, predominately Asian, residential communities in Birmingham - Sparkhill and Washwood Heath - with overt and covert CCTV and ANPR cameras. It was initiated in late 2007 by the West Midland Counter Terrorism Unit (WTU) in the context of a heightened security threat following the discovery of an unexploded car bomb in London, and a terrorist attack on Glasgow Airport. More specifically, earlier in 2007:

> West Midlands Police had thwarted a plot to kidnap and behead a Muslim soldier. The investigation, known as Operation Gamble, was focussed on a number of mostly

British-born Pakistani men living in Birmingham. The investigation was centred on the areas of Alum Rock and Sparkhill.[35]

The areas of Alum Rock and Sparkhill sit in the Washwood Heath and Sparkbrook districts of Birmingham. According to the 2001 population census, 27,822 people were resident in the 5.2 square kilometres of Washwood Heath ward, 57% of whom were described as coming from the ethnic minority population. Sparkbrook has a population of 31,485, over 70% belonging to ethnic minority communities, in an area of 3.91 Kilometres. In total the project consisted of 216 surveillance cameras covering the two districts, 46 CCTV cameras, 8 of which were covert, and 170 dedicated ANPR cameras, 64 of which were covert.

The rationale for the scheme was outlined in the business case made on behalf of West Midland Counter Terrorism Unit (CTU) to the ACPO Terrorism and Allied Matters (TAM) sub group. It stated:

> "The UK is currently facing the most serious and sustained threat from international terrorism ever known. The threat remains real (Security Level: Severe). The events in London of 2005 demonstrated the need for all agencies to enhance their own capacity and capability; working together requires capability to operate across organisational and geographic boundaries. The West Midlands area contains significant features of vulnerability.
>
> (Next paragraph is redacted)

[35] Thornton, S. (2010) *Project Champion Review: An independent review of the commissioning, direction, control and oversight of Project Champion; including the information given to, and the involvement of, the community in this project from the initiation of the scheme up to 4 July 2010*; Thames Valley Police.

> The opportunity to capture data 24/7 instead of an "as and when" basis represents a step change. Deployment decisions based on an absence of knowledge or decisions based on assessments of risk (which may or may not be complete) concerning safety of personnel and the real and potential risks of operational compromise arising from traditional methods, are all drivers for developing the "stand off" options that Project Champion has been developed to deliver."[36]

It outlined the core vision as:

> Creating a 'net' of ANPR to capture target vehicle movements of subjects entering, leaving or within two distinct geographical areas within the city of Birmingham.

And:

> "Delivering an infrastructure for data capture and retention that will add value locally in respect of current operations in the short, medium and long term and available for analytical use in current and future operations on a local, regional and national level.[37]

On the basis of this case, which also suggested that financial support would be forthcoming from Birmingham City Council, ACPO agreed to fund the scheme to the value of 3 million pounds. Because of the sensitivity of the proposals, it was agreed the project should be conducted on a 'need to know' basis and, according to the minutes, this was backed up by more formal actions:

> "The project had insisted on SC [security check] clearance for the Project Manager/ Bid Team and minimum vetting process for contractors. Indoctrination of personnel

[36] ACPO Strategic Outline Business Case - ACPO TAM Business Area, available at: https://www.whatdotheyknow.com/request/36626/response/117902/attach/3/Disclosed%20information%20West%20Mids%20Business%20Case.pdf, page 3.
[37] ibid

has also taken place, together with signing the Official Secrets Act, copying of documents will not be permitted."[38]

Had the scheme limited itself to a covert operation run by the West Midlands Counter Terrorism Unit, it is unlikely that we would have ever known about its existence. However, since the scheme's success seems to have been predicated on a blanket coverage of all vehicle movements, with additional CCTV images of drivers and pedestrians, along dozens of streets, the sheer number of cameras and the infrastructure required to support them could not have been put in place covertly. It was therefore decided to 'piggy-back' the scheme on an expansion of the already existing overt CCTV scheme in the neighbourhood, and market it as a solution to the existing crime problem in the area. As a result:

"the involvement of the CTU took a back seat and the Project moved forwards as a Safer Birmingham Partnership crime reduction / community safety initiative. CTU insignia were replaced by the Safer Birmingham Partnership (SBP) logos and an 'open document' was produced as a brief on Project Champion."[39]

The 'open document', which was widely circulated in the community and used as a briefing document for local councillors, stressed that the scheme was overseen by the Safer Birmingham Partnerships, and that the cameras would specifically address serious acquisitive crime, serious violent crime, violent extremism, and anti social behaviour. It went on to state that it had been funded by the Home Office, and to pose the question:

"Has this anything to do with preventing acts of terrorism?"

To which it gave the answer:

[38] Birmingham City Council (BCC) (2010*) Project Champion: Scrutiny Review into ANPR and CCTV Cameras*, Birmingham City Council, 02 November 2010, page 7.
[39] Thornton, S (2010) op. cit., p. 17.

> "This is not the focus of the operation. The cameras will be utilised to tackle all types of crime to help keep our communities as safe as possible."[40]

This was reiterated by The Assistant Chief Constable at a meeting with local councillors, the minutes of which record:

> "ACC Hyde responded that if he said that additional CCTV and ANPR facilities would not have any benefit around Counter Terrorism then he would be lying and that is why this element was including [sic] in the briefing note however the reassurance and crime prevention benefits are far greater."[41]

The problem, of course, with all these statements is that they were simply untrue. The scheme was first and foremost a counter terrorism scheme, funded by ACPO, not the Home Office, under their Terrorism and Allied Matters Sub-committee, and implemented by the West Midlands Counter Terrorism Unit.

As Thornton's review concluded:

> When the cameras went live at the completion of Project Champion (scheduled for May or June 2010) there would have been no local facility to view the cameras and nobody in place to monitor them.[42]

Indeed, from the outset, the implementation team had agreed that:

---

[40] Councillors Briefing note produced by The Safer Birmingham Partnership available at https://www.whatdotheyknow.com/.../Cllrs%20Briefing%2022.1.10.doc
[41] BCC (2010) op. cit., p. 3.
[42] Thornton (2010) op. cit., p. 30.

> "In consultation with WM CTU it has been agreed that the Champion system will remain independent of the existing Local Authority CCTV environment with the possible exception of sharing power supplies and the mounting of CCTV cameras on existing Council CCTV poles. In these instances, the CCTV cameras will operate over the WM CTU transmission solution."

And:

> "It is understood that the CCTV images captured by the Champion CCTV system are not going to be accessible to partners such as Birmingham City Council as such access could result in an operation becoming compromised.[43]

In January 2010, work began on installing the cameras, which involved digging up the roads and pavements to install the cabling and to erect the 'supersized lamp-posts' necessary to hold the cameras. By April 2010, as local residents became aware of the size of the scheme, opposition started to mobilise and, in May, the project risk register was updated to note that:

> Following the installation of the CCTV poles public and political reaction and pressure has become pronounced. This pressure includes calls for poles to be removed or relocated for numerous reasons, including big brother concerns and aesthetics.[44]

On the 4th June 2010, the story broke in the leading national newspaper, The Guardian, under the headline 'Surveillance Cameras in Birmingham Track Muslims' Every Move'.[45] As a result of the mounting pubic disquiet and community anger, on the 16th of June, the Assistant Chief Constable of West Midland Police and The Safer Birmingham Partnership announced that the work on the scheme would be halted and the cameras covered by plastic bags.

[43] ibid. pp. 15-16
[44] Ibid, p. 27
[45] BCC (2010) op. cit., p. 58.

Two inquiries were set up to investigate the issues, the first was commissioned by The West Midlands Police to be conducted by Sarah Thornton the Chief Constable of Thames Valley Police, but also a member of ACPOs Terrorism and Allied Matters sub-committee, which funded the original scheme. The second was by Birmingham City Council. The Birmingham City Council report concluded that Project Champion was "unacceptable in the way it was constructed to target the Muslim community"; that the police had engaged in a tactic to "deliberately mislead Councillors"; and "there was a catastrophic lack of inquisitiveness" from the Police Authority and the Safer Birmingham Partnership both tasked with scrutinising the Project on the public's behalf.[46]

The police enquiry concluded that "from the start questions should have been asked about its proportionality, legitimacy, authority and necessity; and about the ethical values that underpinned the proposal'". [47] Moreover, the report found that the affair had resulted in "significant community anger and loss of trust". And perhaps most importantly, the Chief Constable concluded: "I found little evidence of thought being given to compliance with the legal or regulatory framework". While some saw this as a damning indictment of police practices, what has never been addressed is the role that ACPO's Terrorism and Allied Matters subcommittee had in funding, planning and authorising the scheme. In both enquiries an examination of their role is absent.

II.3.3 Summary

The range of harms which have arisen as a result of ANPR is perhaps a little surprising. With law enforcement agencies keen to demonstrate results, capitalise on efficiencies and show value for money to policymakers, and private companies to offer convenience to consumers, the human rights and regulatory implications of these interventions have been overlooked in every country we have investigated. In Germany, over-zealous police laws were declared

[46] ibid, p 60
[47] Ibid, p 48

unconstitutional and data retention periods severely curtailed, whereas in the UK, over-zealous extensions of ANPR were the subject of wrangling between NGOs, a weak regulator and unaccountable police bodies such as ACPO, although in the most shocking case of Project Champion the practice was curtailed. In Belgium some forms of ANPR are being used without any legal basis whatsoever. Protest against the human rights and privacy related harms of ANPR is evident in all of the cases, but the Slovakian case is most interesting in this respect. Introduced as an element of transport infrastructure and for economic development reasons by the state, its impact on the economic livelihoods in the road haulage sector and environmental quality throughout the country sparked widespread protest, direct action and highlighted, once again, the lack of forethought around the consequences of introducing such a technology.

II.4 Democratic encounters with ANPR

In this section we discuss the nature of democratic encounters with ANPR at the level of governance, participation and co-determination and public engagement.

II.4.1 Governance

In every case study country except the UK there is specific legislation governing the use of ANPR, and in some there are frameworks for regulation as well. However the nature of those laws is often vague and complex, emerging in piecemeal fashion and lagging behind what the technology can do.

In *Belgium*, the legal framework for ANPR is simultaneously outdated and emergent. The main legislation that regulates the installation and use of ANPR in Belgium is the 2007 *Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's*/*Loi réglant l'installation et l'utilisation de caméras de surveillance* (hereafter the *Camerawet*/*Loi Caméras*) and its 2009 amendment. In addition, the use of ANPR systems is regulated by a 1996 law which covers the authorisation and use of automatic devices in road traffic (in particular for the metric standardisation of cameras) and the Belgian Data Protection Act. The *Loi caméras*

and its 2009 amendment are the core of this legislative framework. As it will be explained, although the 2009 amendment clarified some of the key aspects in the regulation of ANPR cameras, ambiguities and doubts about its legality still exist.

The *Loi Caméras* applies to any fixed or movable system of observation whose aim is to prevent, ascertain or detect crimes against persons or assets or offences of the same kind (Art. 2, 4). On the one hand, in 2007 the adoption of the *Loi Caméras* paved the way for the specific regulation of cameras in Belgium and at last provided clear provisions about the installation and use of CCTV. On the other hand, it is not clear how or whether these rules to ANPR cameras. The main legal concern was linked to the fact that ANPR was considered to be *smarter* than other CCTV cameras and hence it was not clear if ANPR cameras could be automatically compared to *normal* CCTV cameras as described in the legislation. In particular, the 2007 *Loi Caméras* did not clarify whether its provisions were applicable to mobile ANPR cameras. There were opposing views on the law and the Belgian legislator tried to amend it to solve the ambiguity. The 2009 amendment introduced the definition of mobile cameras which "allow observation from different places or positions". Although the 2009 amendment made clear that the *Loi Caméras* applies also to mobile cameras when used on occasion of big gatherings, it did not provide any clarification about the use and installation of mobile ANPR cameras in more general contexts. In 2012 the Privacy Commission addressed this ambiguity of the *Loi Caméras* in its Recommendation n. 4. As the Belgian DPA confirmed:

> "*the Loi Caméras establishes that the use of mobile cameras by the police is admitted only in the framework of "big gatherings" (i.e. a demonstration, a rock concert, …). The use of mobile cameras which recognise number plates in order to search for stolen vehicles, suspects, etc. is accordingly problematic, considered the recent adaptation of the Loi Caméras. By contrast, according to the Loi Caméras, the*

use of fixed surveillance cameras which recognise number plates is certainly possible and legally coherent".[48]

Hence, provided that the *Loi Caméras* applies to fixed ANPR cameras, the Belgian DPA invited the government to address the use of mobile ANPR cameras. Further to the DPA's recommendation, a proposal to modify the *Loi Caméras* was formally submitted to the Belgian Senate on 20 June 2013. This new amendment, which is pending approval, will finally make the use of mobile ANPR cameras legitimate under Belgian law. The revision of the *Loi Caméras* is expected in early 2014 and lawyers look forward to a detailed legal framework for mobile ANPR and smart cameras.

Debates about the proposed amendments to the *Loi Caméras* have been going on in the Belgian Parliament since mid-2013. Different opinions have emerged with regards to the design of a new legal framework concerning the use of ANPR cameras by police forces. In particular, two different views emerged. On the one hand, Liberals were more inclined to integrate legal provisions concerning the use of ANPR cameras into the existing *Loi Caméras.* On the other, Christian Democrats wanted to incorporate them into the Police Act. This latter position has prevailed.

A complex situation also emerges in *Germany*. First, the legal basis, on which ANPR operates is multi-layered. ANPR operation may simultaneously fall under a number of spheres of competence and may be supervised by a number of different authorities. Since ANPR can be applied either for crime prevention or law enforcement, the legal basis can be

[48] The text within inverted commas here is an unofficial translation into English of the original French document. The corresponding paragraph of the Recommendation reads as follows: "*la loi caméras prévoit explicitement que le recours à des caméras mobiles par les services de police n'est possible que dans le cadre de ce qu'on appelle des "grands rassemblements" (par ex. une manifestation, un concert rock, …). L'utilisation de caméras de surveillance mobiles avec reconnaissance des plaques d'immatriculation en vue notamment de rechercher des véhicules volés, des personnes signalées, etc. est en d'autres termes de lege lata problématique, vu cette récente adaptation de la loi caméras. Par contre, selon la loi caméras, l'utilisation de caméras de surveillance fixes avec reconnaissance des plaques d'immatriculation est bel et bien possible et juridiquement cohérente*". Privacy Commission, Recommendation no. 4/2012 of 12 February 2012, ibid., para. 53.

found in the police laws of the *Länder* or in the Code of Criminal Procedure (*StPO*, *Strafprozessordnung*) that falls under the responsibility of the federal government. In the latter case the police invokes §§100h, 111, 163e, 163f StPO. And in the former case, when it comes to the deployment of ANPR for the purpose of preventing crime, the legal basis can be found in the different police laws of the *Länder*.

Second – and this point is closely related to the first – the prerequisites for a deployment of ANPR differ depending on the legal basis that is invoked. When the police use ANPR based on the police laws, the procedure actually reflects an automated search for specific number plates (*automatische Kennzeichenfahndung*, meaning an automatic number plate search). Number plates are scanned and immediately matched with tracing files. If a hit occurs the respective action is initiated, if no hit occurs, all collected data is immediately deleted. These strict regulations are a direct result of the decision of the Constitutional Court in 2008. The police use ANPR for several purposes such as: the search for stolen number plates or vehicles, the search for criminals or the detection of car holders that violate the obligation to have liability insurance.

Specific regulations for ANPR can be found in 11 police laws (see Table II.4). Berlin has no specific regulation but uses ANPR and refers to other provisions, and North Rhine-Westphalia and Saxony-Anhalt have never had regulations dealing specifically with ANPR. In Schleswig-Holstein, regulations existed between April 2007 and April 2009, when it was decided to suspend the regulations as a consequence of the Constitutional Court's decision. Up to now, no new regulation has been introduced. The same accounts for Bremen, where a specific regulation existed between March 2006 and July 2008.

Alternatively, when the police use ANPR based on the Code of Criminal Procedure, they are allowed to either use it for an automatic number plate search or as a tool to arbitrarily scan all vehicles driving by with the aim of saving vehicle related data to process it as and when required. This practice is mostly used for observations (*Kfz-Massenscanning* or

automatische Nummernschilderfassung, meaning automatic number plate recording). Contrary to the police laws, ANPR is not explicitly regulated in the Code of Criminal Procedure. Instead, the Code of Criminal Procedure that regulates the conditions under which checkpoints aimed at the identification and detection of criminals may be put in place. Furthermore the use of technical devices for observations is regulated. Thus, the Code of Criminal Procedure offers sufficient enabling provisions for the use of ANPR for observations in specific cases of considerable importance. As we will see later, the facts show that this only happens rarely.

A third factor that serves to complicate the regulatory situation in Germany is that claims against provisions in four *Länder* are currently still pending. Accordingly, the constitutionality of these regulations remains uncertain. Claims against provisions in Lower Saxony, Bavaria, Hesse and Baden-Württemberg had been lodged following the Federal Constitutional Court's decision on provisions in Schleswig-Holstein and Hesse. These claims were a momentous way of engaging with the surveillance practice and the authorities deploying ANPR. The fact that the Federal Constitutional Court – as the highest judicial authority – dealt with ANPR in two *Länder* reflected an important step in the history of ANPR. The Court decision forced the *Länder* to clearly define the requirements under which ANPR is allowed, and therefore supported citizens in their fundamental rights. For instance, by regulating the retention dates and requiring an immediate deletion of the collected data, the Court made a strong case for the citizens.

Land	Specific provision for ANPR?	Where?	Since when does the current regulation exist?	Use?
Baden-Württemberg	Yes	§22a PolG	2008	No
Bavaria	Yes	Art.33 para. 2, p.2-5, Art.38, para. 3, Art. 46, para. 2, p. 4 PAG	2008	Yes
Berlin	No	-	Police refers to other provisions	Yes
Brandenburg	Yes	§36a BbgPolG, §100 h stop	2006	Yes
Bremen	No	Regulation existed between 2006 and 2008	-	No
Hamburg	Yes	§8a HmbPolDVG	2012	No
Hesse	Yes	§14aHSOG	2009	Yes
Lower Saxony	Yes	§32, para. 5 Nds. SOG; §§100h StPO, §111StPO in conjunction with §163 d StPO.	2009	Yes
Mecklenburg-Western Pomerania	Yes	§43a SOG-M-V in conjunction with §47 para. 2 SOG M-V, §18 para. 1 DSG M-V.	2006	Yes
North Rhine-Westphalia	No	-	Police refers to StPO	Yes
Rhineland-Palatinate	Yes	§27 para. 5 p.1 RhPfPOG	2011	n/a
Saarland	Yes	§ 27 para. 3, SaarlPolG	2007	No
Saxony	Yes	§19a SächsPolG	2011	Yes
Saxony-Anhalt	No	-	-	No
Schleswig Holstein	No	Regulation existed between 2007 and 2009	-	No
Thuringia	Yes	§33 para. 7 in conjunction with § 14 para. 1 Nr. 2 - 4 ThürPAG	2008	No

Table II.1: Legal provisions for ANPR in the Länder of Germany

In practice, the 16 *Länder* handle the Court decision differently which makes the deployment questionable in terms of constitutionality. This becomes obvious by the fact that currently claims against provisions in four *Länder* are pending. In addition, those who handed in complaints are not satisfied with the decision, since they regard the scanning and analysis of the number plate, in itself, as a violation of basic rights. This issue is crucial to the legal assessment of ANPR. The right that is of particular relevance in the German context is the right to informational self-determination (*Recht auf informationelle Selbstbestimmung*).

The right to informational self-determination is a right that is not explicitly anchored in the German constitution, but is derived from another fundamental right, the *allgemeine Persönlichkeitsrecht*. It is rooted in a judgement that passed in 1983, the so-called *Volkszählungsurteil*. In this judgement, it was decided that the *allgemeine Persönlichkeitsrecht* also protects the right of the individual to decide when, and within which boundaries, personal information is disclosed. The right to informational self-determination is supposed to protect the right to decide about the use of personal data in the face of developments in information technology and the new possibilities they threw up in the collection, storage and processing of data.

The practice of ANPR infringes upon the right to informational self-determination as soon as the collected data is stored. If the data is deleted immediately, for example in case of a non-hit, no intervention in the right to informational self-determination is perceived. Drawing on the decision of the Federal Constitutional Court in 2008, the following aspects are prerequisites for the regulation of ANPR in the police laws (or, to put it in another way, the conditions under which an intervention in the right to informational self-determination is acceptable):

2. Sufficiently precise enabling provisions for the respective measure are necessary, i.e. occasion, purpose and limits of the use of ANPR have to be stated clearly.
3. If ANPR is applied, it has to be proportionate, i.e. the enabling provisions have to take account the different uses of ANPR and their respective degrees of intervention. The degree of intervention depends on several factors; such as the occasion and the amount of data collection, the affected group of people and the intended use of the collected data.

According to two comprehensive studies which investigated the constitutionality of the police laws, some provisions are at least questionable in terms of constitutionality. In those two

studies, the different provisions are systematically investigated by referring to the above-mentioned prerequisites. Some *Länder* met the requirements in large parts, some needed improvement, and some were not compatible with the constitution.

When ANPR is used to administer road tolling its legal basis is different again. It can be found in the BFStrMG (*Bundesfernstraßenmautgesetz*), which defines what kind of vehicles are obliged to pay on which streets. Furthermore it regulates how the toll is collected and the quality assurance systems required to ensure that tolls are paid correctly.

According to the BFStrMG, two types of data are allowed to be collected during the procedure of the collection of the toll: one is related to the route a truck is taking, the so-called *Fahrtdaten*. It includes the street charge that has been paid, the distance the truck has been paid for, the place and time of toll payment and the number plate. In addition, the toll relevant attributes of the truck are collected, i.e. the amount of axles, emission class and weight. The operating company, Toll Collect, deletes the route related data after 120 days, and the Federal Office for Goods Transport stores the data for six years. The number plate has to be deleted after three years.

A second type of collected data is the control data (*Kontrolldaten*). It includes a picture of the vehicle, the name of the person driving the vehicle, place and time, number plate and the toll relevant characteristics of the vehicle that is charged. Control data is only allowed to be used for the monitoring of compliance with the rules of the BFStrMG. It is prohibited to transmit or use this data. Rather, it has to be deleted immediately after it has been ascertained that the vehicle is not obliged to pay the street charge or that the toll charge has already been paid. If the toll hasn't been paid, a charging process has to be initiated and Toll Collect has to delete the data as soon as the charging process has been completed. The Federal Office for Goods Transport stores the data for two years.

What stands out in the German case is the strong top-down control of ANPR: A look at the legal situation in Germany reveals that the Federal Constitutional Court clearly defined restrictive prerequisites for the use of ANPR by the police. Interestingly enough, as the reaction of the *Länder* shows, there is obviously room for interpretation about how exactly the Court decision feeds into the police laws of the *Länder*. As a matter of fact, the *Länder* reacted differently to the Court decision. This is reflected in the variations in current regulations and practices. These different developments are highly contested – which is reflected by the pending claims against ANPR provisions in different *Länder*. Hence, controversies surrounding ANPR are obviously not resolved. There is still a high degree of uncertainty about the constitutionality of ANPR use that leads to very reluctant behaviour on the part of the main actors.

In *Slovakia*, the legislative framework invokes a number of different statutes pertaining to different aspects of the infrastructure. The framework legislation for electronic toll system, the Law No. 25/2007 *Coll. on Electronic Toll Collection for the Use of Specified Sections of Ground Roads* was approved by the Slovak parliament at the end of 2006. The law established the basic conditions for the introduction of ETS in Slovakia and allowed for public procurement for a system operator. The law also implemented two EU directives, 2004/52/EC on Interoperability of Electronic Road Toll System in the Community and 1999/62/EC on the Charging of Heavy Goods Vehicles for the Use of Certain Infrastructures.

The governance of the ETS is intertwined with other laws, e.g. *Law on the Railway Police*, of which the Toll Police is organizational unit or the law *No. 315/1996 Coll. on the Road Traffic*, in which toll offences are defined. Besides the main ETS law is also implemented by various executive legal acts, e.g. *Regulation of the Government No. 350/2007* Coll. stipulating the toll rate amount for the use of specified sections of ground roads, *Decree No. 388/2009 Coll. (Toll Order) of the Ministry of Transport, Post and Telecommunications* governing details of toll collection or decree No. 441/2011 Coll. of the Ministry of Transport, Post and

Telecommunications that specifies the sections of highways, expressways and the 1st class roads in the toll system.

Since its approval in 2006 the main toll law was amended 11 times, mostly by indirect amendments. This is not unusual in the Slovak legal system, especially if the original law was approved full three years before the ETS was launched into the service. It is interesting that the Slovak Data Protection Agency did not comment on the privacy, rights or surveillance aspect of the legislation at any point, nor was it discussed in the media.

A significant change was made in November 2013 to protect minor roads from the damage caused by heavy good vehicles. This law extended the toll system to 2nd and 3rd class roads, introduced absolute liability for toll offences and increase of fines for toll offences. The Ministry of Transport plans to use a zero-toll on 2nd and 3rd class roads for aggregation of precise data "about movements of trucks in individual regions"[49] and evaluate this data every six months. This new law also introduces several other changes which are relevant for the surveillance aspect of the ETS. First, the law lists the kind of data the ETS operator, or third parties can collect and process. Secondly, the access to the data from ETS is to be granted not only to the Police and SIS, as it was until now, but also to Financial Administration and Military Intelligence. Both changes were submitted during the consultation phase at the governmental level by Interior Ministry and Defense Ministry. Moreover, the phrasing of the section does not limit the use of the access to toll offences only, as it was in 2007 law. As it was case with the previous 2007 law, proposals to grant access to ETS data for other enforcement agencies did not get any attention by the media or in later phase by the parliament. Thirdly, the new toll law introduces "absolute" liability for toll offenses in order to increase the enforcement.

[49] See Slovak Spectator, 21/10/2013, Changes To Electronic Toll System, available at: http://spectator.sme.sk/articles/view/51739/23/changes_to_electronic_toll_collection.html, accessed 16/12/2013

The final change brought by the law is not technically part of the law itself. The impact assessment report attached to the draft of the law announces that the new Central Registry for Offences will be established for administration of traffic offences. It will serve primarily as a registry for toll offences, but the report acknowledges that it is going to be used also for other traffic offences and vehicles, outside of the ETS framework, e.g. speeding, reckless driving. In other parts of the report it is explicitly acknowledged that the registry will use data gathered by the existing technical infrastructure that is part of ETS enforcement system (e.g. portable and stationary gates, camera systems, radar and laser systems). No other details are yet available on the Central registry. The establishing of Central registry will therefore solve the last problem before introduction of wide surveillance of the vehicles on Slovak roads, as both legal framework, and the technical infrastructure will be in place. Current law concerning the collection of and access to data is described in the next two paragraphs.

There are two types of data that are collected within the ETS. First, the electronic data that is collected by the toll operator, i.e. plate number, the technical properties of the vehicle, the identification code of on-board unit ("OBU"), the distance driven on the toll road, the toll rate and information about the vehicle's operator. The second type of data collected is vehicle registration data. While there is a specific document on data protection provided by the Toll operator (SkyToll) , it only covers the fact that the data controller of the ETS is the NDS ("National Highway Company), that the data processor is the SkyToll and that the third parties are involved with distribution of OBU units, and therefore, with personal data. While the type of data collected within the ETS is explicitly listed by both law, and legal contracts provided by the SkyToll, the data retention is limited by the (very general) data protection law. The only explicit period mentioned in the documents is that the drivers' personal data are deleted six months after collection if a toll contract is not renewed. When SkyToll was

specifically asked about the retention of data which was collected at the toll gates the response was that the information is "confidential". [50]

The comparison of the first draft of the electronic toll law, as discussed by the government in February 2006, with the current wording of the law as of December 2013 shows one important difference. The current law, i.e. §6(7) obliges the ETS operator *to grant live and direct access to all data collected within ETS to the Police and Slovak Information Service (SIS, intelligence agency)*. This is missing from the 2006 original draft. The proposal to grant access to ETS to the Police was submitted during the second reading of the toll law in December 2006 by coalition MP Mr. Pelegrini, together with several other changes he proposed to the draft. His reasoning was that "the Police needs to control the enforcement of the law, therefore it needs to have an access to ETS data".[51] Although in reaction to his proposal one MP from opposition raised a suspicion that the extensive proposal was in fact prepared by the Ministry of Transport, as it is often the case, the Minister L. Vážny refused to acknowledge this. The proposal to grant the access to ETS was approved by an absolute majority of MPs (120 out 150).

A year later, in 2007, the Transport Ministry prepared an amendment to the Law on Railway Police in order to establish the Toll Police as an organizational unit. During the consultations on the draft two of the country's intelligence agencies, SIS and Military Intelligence individually proposed an amendment to grant them live and ongoing access to data from ETS. Both demands shared similar arguments, pointing to agencies legal obligations and duties. Only SIS however produced elaborate explanation that argued that direct access to ETS data (e.g. license plates, pictures, localization data, time data) was essential during intelligence operations and could not be substituted with indirect access, as this would

[50] ibid

[51] See Transcipt of the Session of the Parliament, December 2006, 13/12/2006, available at: http://www.nrsr.sk/dl/Browser/Document?documentId=164072

"objectively cause noise and faulty data".[52] The Transport Ministry accepted only the proposal by the SIS and the amendment was approved in the parliament in 2008, the Law No. 86/2008 on the Railway Police.

The general Data protection law regulates the subject access request to ETS data. The aforementioned document on privacy that is available on the website of the EMyto.sk (E-Toll) just mentions existence of the subject access request, referring to the DP law. However, no templates (online or printed) for requests are available. As for the usage of the right, no public data were available. According to the response from the Slovak DPA, there were no complaints made to the DPA about by legal subjects about the ETS.

In the *UK*, there is no specific legal framework for the use of ANPR. Instead, its use has slowly diffused in a way which has circumvented parliamentary scrutiny. As we have already discussed, if cameras are covert they are regulated by the Regulation of Investigatory Powers Act (2000) because they constitute 'directed surveillance', but other than that, it can be challenged using the provisions of the Data Protection Act. Its history dates back to the 1970s. Here is a brief history of the police development and deployment of ANPR technology:

- 1976: The Government's Home Office Scientific Development Branch began working on the development of ANPR Technology.
- 1980: It was reported in the Annual Report of Her Majesty's the Chief Inspector of Constabulary that a field experiment was to be conducted to test the viability of automatic number plate reader technology being linked to the Police National Computer. The main use was declared to be the identification of stolen vehicles.
- 1982-84: Between July and October 1982 police-sponsored trials occurred at the approach to London's Dartford Tunnel road crossing of the river Thames. These

[52] Available at: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-77415?prefixFile=m

were superseded by trials of a more advanced system on the main national motorway, the M1, which could match a number plate against the database of suspect vehicles in 15 seconds. Further work was being undertaken to reduce the time to complete the matching process to one second.

- 1996: The City of London's 'Ring of Steel' was the first major application of ANPR as a counter terrorism measure. It was set up in the wake of the Bishopgate's bombing, which killed one person, injured forty and caused hundreds of millions of pounds worth of damage in the heart of London's international financial district. Rather than 'steel', the system consists of cameras situated at each of the entry points into the City. Since 1996, every vehicle that enters the square mile of the City of London has had its licence plate read by the cameras. This information is then automatically checked, in real time, against a number of databases that contain details of the vehicles of suspected terrorists. If a match is made, an alarm is sounded and officers can be deployed to investigate the suspicious vehicle further.
- 2001-02: Project Spectrum - In response to the 9/11 bombing of the World Trade Centre in New York and the subsequent war on terror, the first nationally co-ordinated deployment of ANPR in England and Wales was initiated. Under the Crime Reduction Programme the Home Office allocated £4.65 million to provide each force in England and Wales with one mobile ANPR unit and associated back-office facility.
- 2002-03: Project Laser was a six-month pilot of fixed ANPR cameras in nine police forces. The aim of the pilot was to gather information on the operation and impact of ANPR-enabled intercept teams, to inform policy and assess the potential of a national roll out. In the trials, the teams "stopped 39,188 vehicles, arrested over 5000 persons (of which only 20% were for driving related matters) and took a further 45,000 actions. These included issuing verbal advice or a fixed penalty, or requesting that vehicle documentation, such as MOT certificates and vehicle insurance, be presented at a police station".

- 2003: London Congestion Charging introduced to central London. The area in which charges apply is a zone measuring 21 square kilometres with a total of 203 entry and exit points. Road signs alert motorists when they enter the charging zone. There are no tollbooths, barriers or tickets - instead, drivers pay to register their vehicle number plates on a database, and a network of nearly 700 cameras records their entry into, movements within and, exit from the zone. The number plates are matched against the database. If a vehicle is registered as having paid by midnight on the day of travel, then the data is erased. If the vehicle is identified as having not paid the charge then the registered owner is automatically sent a fixed penalty notice. The address is obtained from a link, which provides access to the DVLA database of registered keepers.
- 2003: Project Laser is extended and the pilot study increased to 23 forces, part-funded by money from the fixed penalty fines generated from motoring offences captured by the system. During the 13 months of Laser 2, "ANPR cameras read approximately 28 million VRMs of which over 1.1 million (3.9%) resulted in a hit. In total, the ANPR intercept teams stopped 101,775 vehicles (9.2%) of these vehicles as a result of ANPR hits".[53] According to the, then home secretary, David Blunkett, the outcomes from the pilot were impressive and the "Home Office estimates that a national roll-out of ANPR would lead to approximately 24,400 additional offences being brought to justice each year – a significant contribution of around 15% towards meeting the Government's target for offences brought to justice."
- 2005: The Association of Chief Police Officers (ACPO) published their National ANPR Strategy "Denying Criminals the Use of the Roads" 2005/2008.[54] The strategy consisted of four key components: the setting up of a national network of ANPR-capable cameras; the creation of dedicated intercept teams in each force; real time

[53] PA Consulting (2004): PA Consulting (2004) *Engaging criminality – denying criminals the use of the road*, PA Consulting Group, London. p14
[54] ACPO - Association of Chief Police Officers – (2005) ANPR Strategy for the Police Service 2005-8: Denying Criminals the Use of the Road, London ACPO

linkages with the DVLA database of registered keepers of motor vehicles and to the databases contained on the Police National Computer (PNC); and the creation of a National ANPR Data Centre to house a database capable of storing 35 million ANPR reads per day.

- 2007: The Home Secretary, Jacqui Smith, granted The Metropolitan Police force and Transport for London exemption from the Data Protection Act to allow the real time transfer of data from the London Congestion charge system to the Metropolitan Police. Police were previously able to request specific footage from those cameras for reasons of national security. However, given that data is erased once payment has been confirmed, this limited the potential use for police purposes. The certificate allowed for the blanket transfer of real time data to be stored and processed by the police but only for the purposes of matters of national security and not for general policing purposes.

Unlike in other European countries, the UK police national ANPR network is not used to enforce speed restrictions despite the fact that ANPR cameras are ideally suited to calculating the average speed that a vehicle travels between two points on the road network. To understand this, we need to review the contentious history of camera-based speed enforcement in the UK. The 1991 Road Traffic Act allowed, for the first time, evidence collected on camera to be used in the prosecution of motorists for speeding or red light offences. However, throughout the 1990s, camera enforcement remained limited since the 'cost of installing and maintaining speed cameras in the 1990s meant that some police forces had only one in eight devices operating at any one time and drivers were beginning to realise that they were unlikely to be caught.'[55] In 2000, the government sponsored a pilot Safety Camera Programme, which allowed for the income derived from fines to be retained in eight pilot areas and to be used pay for the costs of enforcement and other road safety

[55] Louise Butcher, (2009) 'Roads: Speed Cameras', *House of Commons Briefing Paper*, Standard Note:
London, House of Commons Library, p. 5.

activities. In 2001, legislation was introduced that allowed the system to be rolled out nationally. The effect was a dramatic rise in the number of enforcement cameras: from 1,935 in England and Wales in 2000 to 5,562 by 2006 and, by 2009, the number had increased to around 6,000. Correspondingly, the number of prosecutions and fixed penalty notices arising from camera-based enforcement of speeding and red light infractions increased eight fold between 1995 and 2005, to a total of just over 2 million. As a consequence, the surveillance of motorists for the purposes of enforcing road traffic law has been one of the most politically contentious surveillance measures, with national newspapers, opposition ministers, and pressure groups accusing the government of trying to criminalise the motorist, exaggerating the beneficial effects of speed cameras and generating a stealth tax through the collection of fines.

II.4.2 Participation

When considering wider participating in the shaping of ANPR, the activities of peripheral stakeholder groups are examined in terms of the shaping of the practice. These peripheral stakeholders include system suppliers, regulators, parliament, local government, the media and NGO/activist groups. We find low levels of participation in relation to these wider stakeholders. The development and operation of ANPR systems is largely a result of public private partnerships, with large amounts of public spending involved. This is a particularly novel approach in *Slovakia*. The ETS system installation was the first to test the public-private partnership funding model which has since been extended to a number of public infrastructure projects. Furthermore, because of the financial and economic focus of the debates surrounding the system, there has been little opportunity for the more critical stakeholders, such as the DPA, the Courts and NGOs, to state their concerns about the project.

The stresses associated with ANPR in the last section highlighted how, in certain circumstances, the operation of ANPR was influenced by state legal and regulatory

processes. In the *UK*, the Information Commissioner and the Surveillance commissioner are involved up to a point but have rarely, if ever taken radical action to curtail some of the more problematic uses of ANPR in that country. In *Belgium* there are different ways in which public authorities and the local and federal police forces could be made accountable for the installation and use of ANPR cameras. However, these accountability strategies seem to be ineffective at present. The *Loi Caméras* does not ask for any kind of evaluation or public accountability of a camera system. For fixed ANPR cameras, however, advice from city councils is obliged by law. The new *Loi Caméras* will include a legal framework for mobile ANPR cameras, accountability mechanisms might involve the Belgian Ministry of the Interior or the council of the respective local police force. In turn, decisions about employing ANPR surveillance would be shifted towards higher-scale councils of local police forces which have almost no link with 'ordinary citizens'.

In *Germany*, ANPR has been the subject of parliamentary debate as well as legal action and limitations. Politicians – mainly from the conservative party – regularly call for the toll system to be used to trace criminals. They argue that it is necessary for effective police work and that this would lead to an increase in security. Some politicians also hold the view that it is irresponsible not to use the available data, and difficult to justify why the data is not used. They argue that in the case of non-use, the perpetrator is protected instead of the victim. In the course of the introduction of a number of counter-terrorism laws in 2007 ("*Schäuble-Katalog*"), the federal ministry of the interior argued that the toll gantries should be used for crime prevention and law enforcement. Minister Schäuble stated that the importance of effective law enforcement outweighs that of data protection in the case of serious crime and terrorism. The Federal police also welcome a suspension of the purpose limitation principle. They say law enforcement would be facilitated and if the use is only limited, the danger of total surveillance does not exist. Contrary to this, the Data Protection Commissioners for the *Länder* are against the use of toll data for law enforcement. They argue that the high error rate of the system, the disproportionality of the measure and the danger of total surveillance

are problematic. Even if the use is at first restricted to serious crimes, it might easily be expanded to other kinds of crime. Further, it might be difficult to argue why only truck drivers should be surveilled and not every vehicle. In addition, they do not see a necessity for this tool to be used by the police.

II.4.3 Engagement

The notion of public engagement with ANPR is difficult to establish in three out of four of the cases (Belgium, Germany and the UK) because of low public awareness of ANPR as well as, in Belgium, Germany and the UK, ANPR is not required to be signed. In Slovakia, however, because of the economic impact of its ANPR based toll system, there is widespread public awareness of ANPR and significant engagement with it. Furthermore, as ANPR systems are implicated in the creation of 'data doubles' – electronic records of the identity and activities of individuals in a particular place and time – individuals may engage with this data after their encounter with ANPR through subject access requests under data protection legislation. We now discuss each case in turn. In particular, we discuss how media coverage has engaged public opinion on ANPR as it would be instrumental in raising public awareness of it.

In *Belgium* the media have been reporting on ANPR since around 2005, but coverage has intensified since 2011. News about the installation of new ANPR cameras is reported on a regular basis, particularly in the Flemish press. The coverage has generally been positive. Throughout Belgium, the media have highlighted the added value of ANPR as smart cameras, emphasising the views of public authorities and private companies. Generally the press do not refer to privacy and to the impact of ANPR on fundamental rights and freedoms, although this has begun to change more recently. Similarly, arguments concerning the risk of the function-creep seem to be mainly disregarded by the media. Indeed, the lack of a proper public debate on the use of ANPR is still a matter of concern. However, it is important to note that the press has mentioned about the lacunae of the

national legislative framework since 2009 while envisaging amendments to the provisions of the *Loi caméras*, in particular with regards to mobile ANPR cameras.

In *Germany*, the newspaper most frequently covering ANPR was the national daily *Sueddeutsche Zeitung* (18 articles) followed by *Frankfurter Rundschau* (11 articles), other national dailies and several regional newspapers (*Der Tagesspiegel*, *Stuttgarter Nachrichten*, each 10 articles). Of the web based publications, *Spiegel Online* (5 articles) and *sueddeutsche.de* (4 articles) were the most relevant. Coverage tended to peak in response to major events connected to ANPR deployment. The most significant event is the decision of the Constitutional Court in 2008, which is covered in most of the articles. Smaller peaks are caused by various criminal cases where truck drivers are involved – the most recent one was the 'truck-sniper', where a truck driver fired haphazardly on other trucks using a variety of small arms weapons between 2008 and 2013.[56] The case was solved in June 2013 by using ANPR, which led to a short news peak. Generally speaking, the number of articles per year decreases sharply after the constitutional court decision in 2008.

Concerning ANPR for crime prevention and law enforcement, the police and the Ministries of the Interior of the *Länder* are uncommunicative in terms of public engagement. It seems that the increase of security through the use of ANPR is more important than the democratisation of the system. This position became quite obvious in June 2013, when the Federal Police released that they have been using ANPR for a couple of months to find a suspect. This was only made public only after they found the suspect with the help of ANPR. Obviously, the police see it as an advantage if the locations of the ANPR cameras are not known. Hence, engagement with the public happens only occasionally, and in a reactive manner, or when the authorities claim the use as a success.

[56] http://www.telegraph.co.uk/news/worldnews/europe/germany/10139207/German-motorway-sniper-arrested.html

In *Slovakia*, the case is somewhat different. The media have played a significant role in fuelling public debate about the ETS system as well as the introduction of ANPR Into police vehicles. "Police cars of the future", "Police to drive intelligent cars",[57] are only two of many headlines from Slovak media that informed the public, in November 2013, about the latest developments. Media reports in the testing phase of the technology reported that in pilot testing police were overwhelmed as the system delivered hundreds of hits. The media also reported that several private companies were testing their technologies, probably preparing for the public procurement.

In relation to the ETS, the media have been key in reporting the economic impact and the economic motivations behind the toll system, which was regarded as a state financial levy by all involved. The media were key in highlighting the experiences of villagers whose environments had been ruined by heavy commercial traffic, and in reporting the Dvorianky villagers campaign to have signs installed. The system was introduced to increase budget revenues; the operator of the system, a private company that operates system is motivated by the profit. The subjects of the toll, haulier companies and drivers use various techniques to avoid ETS, but their motivations are also financial. Critical events and responses to the ETS are motivated by the costs, not privacy. Because of this, personal data and the privacy is missing altogether from legal, political and public discussions about the ETS. No public data are available on how often ETS data are accessed by Police or security services. Also, the media did not find any article in which the Police acknowledged the use of ETS data for its operations. The same question was asked of the police during the course of this research but no response was obtained.

In *Britain*, certain sections of the press are hostile to ANPR because of its economic implications, reflecting the situation in Slovakia. Local authority use of ANPR is now a

[57] See for example: SME, Polícia bude jazdiť na inteligentných autách (Police will drive intelligent cars), 20/09/2013, available at: http://auto.sme.sk/c/6941905/policajti-budu-jazdit-na-inteligentnych-autach.html, accessed 09/10/2013

subject of much hostile journalism. For instance, under the headline, 'Those sneaky council spy cars fleece drivers of £32million a year... but now motorists are fighting back', *The Daily Mail* newspaper reported*:*

> that in the 12-month period between November 2012 and October 2013, more than 110 spy vehicles used by councils in England and Wales resulted in 330,000 penalty charge notices for parking offences and so-called 'moving traffic violations'. These would have raised £32 million, if paid in full.[58]

However more left wing sections of the press, particularly The Guardian Newspaper, have been instrumental in highlighting government surveillance practices, particularly those of the NSA and GCHQ and their impact on human rights. They criticise the police's use of ANPR and its utility to government, and have aided SJ Mathiesen in his attempt to uncover the location of ANPR cameras. As we mentioned earlier, attempts in the UK to engage with ANPR using Freedom of Information requests struggle to uncover anything useful. ANPR locations, as a national security technology, were deemed to be too sensitive to reveal to the general public.

Therefore, it has to be concluded that law enforcement agencies do not engage with the public over ANPR matters and the public do not generally know the terms of their engagement with ANPR. Press coverage occurs occasionally if there is anything newsworthy about ANPR practice, particularly if it raises controversy. The places where discussions about the pros and cons of this surveillance technology occur are in policy arenas. Representatives of different pressure groups and scientific experts are given a say in policy-making processes – at least formally. In principle, it is possible to trace those political discussions through publicly available parliamentary documentation. In practice, however, this is only done by a very small fraction of society. Those who actually engage

[58] http://www.dailymail.co.uk/news/article-2597460/Those-sneaky-council-spy-cars-fleece-drivers-32million-year-motorists-fighting-back.html

themselves show a special interest in surveillance and data protection related topics i.e. those who handed in constitutional complaints, activists and political commentators.

II.5 Improving democratic resilience in the face of ANPR

Across the cases we see variation in the use of ANPR along key contextual parameters highlighted in WP2. First we see the influence of contrasting legal frameworks which embody different rationales for the use and scrutiny of ANPR. Germany's top down regulatory approach coupled with scrutiny by the courts and parliament contrasts sharply with Britain's extra-regulatory use, media scrutiny and challenges under the data protection regulation. Belgium's emergent regulatory framework emerges as a mid-point between the cases of Germany and the UK, and Slovakia's economic rationale on the back of which surveillance and security issues are conveniently packaged and data protection and privacy are conveniently side-lined. Media coverage focuses on controversies and the media tend to be split into pro- and anti-governmental camps. As a law enforcement technology it is not surprising that in each country security discourses are mobilised in favour of ANPR whilst privacy and data protection discourses are mobilised against it. In the UK in particular, security discourses are used to silence opposition to the practice and to trump democratic rights, particular those relating to FOI requests. In Slovakia security, surveillance and privacy discourses are barely circulating in the public sphere at all.

Concerning the question of how democratic resilience could be improved in the face of ANPR, we must first consider whether the harms we have discussed in section II.2 of this report are recognised in the different case study countries.

In *Belgium*, the lack of a legal basis for mobile ANPR has been recognised with recent legal changes. These legal changes also allow for a consultative framework over the implementation of ANPR. More broader issues surrounding privacy, consent and notice that ANPR cameras are present have not been addressed, however.

In *Germany*, a robust rights framework surrounding information self-determination and a constitutional court to which citizens can make complaints about the constitutionality of various government practices have ensured two things. First, that the harms of ANPR are recognised and second, that legal limits to the use of ANPR are put in place. Germany has a strong, top-down regulatory framework for ANPR governance. It has also been the subject of parliamentary debates. However there is still low general public awareness of ANPR and the organizational practices and processes surrounding its use have been criticised for being transparent.

In *Slovakia* the economic and environmental harms which stem from the ETS mirror the reasons for which it is implemented: economic revenue collection and the regulation of road use. The environmental consequences of this have been counteracted with an extension of the ETS to cover a wider range of roads coupled with no entry signage. No public discussion of the harms associated with privacy or surveillance has occurred and there is no public acknowledgement of the issue. In spite of this security services and police have access to ETS data. Furthermore subject access rights are not encouraged. Data Protection Authorities have not mobilised their powers in relation to the ETS.

In the *UK* ANPR is on the public agenda but some of the significant harms which have been witnessed in the UK have not been counteracted in an official level. This is partly because it is not governed by a specific law and its governance not subject to specific scrutiny. ANPR's impact on the right to protest peacefully, its overall transparency, its impact on privacy as expressed through data protection legislation have each hit the headlines as the subject of democratic wrangling between regulators, activists and the police. One particular shock was quickly counteracted and exposed some of the obfuscatory and deceitful tactics used to deploy extensive surveillance on the muslim populations. Democratic tools such as FOI have proven ineffective in revealing more about ANPR practices and creating some transparency and accountability surrounding it. In the British context, however, there is active public debate on surveillance and high public awareness of the surveillance society in general.

In order to strengthen democratic resilience in the face of ANPR, we would argue that increased public awareness of ANPR through signage and through media coverage would help. This in itself would fuel NGO activism against ANPR which has been effective in a number of contexts. Public information about ANPR systems, clear reporting on the effectiveness of the systems and public accountability mechanisms through which the watchers could be watched are required. Data protection authority powers would also need to be strengthened. Active tendering for new ANPR systems which emphasised privacy by design might also be a way forward.

CHAPTER THREE

CREDIT SCORING

III.1 Credit Scoring: An introduction to the practice

Credit Scoring is a surveillance practice whereby financial services companies who are lending money calculate the creditworthiness of their customer. A customer's credit score helps to determine whether a loan should be made and the interest rate that is offered. The origin of credit scoring and credit checking is decades, if not centuries, old and one widely circulated story in the credit scoring literature tells of its emergence. In a small 19th century American town, a number of shopkeepers who had granted credit to a customer began to converse. The customer in question frequented their stores and had secured credit from all of the shopkeepers. When the shopkeepers realised they had all granted credit to this customer and that his repayments were less than forthcoming the customer's reputation suffered and he failed to receive credit again. The workings of this story are conditional on localized knowledge, where populations are relatively intimate. Within less intimate surroundings assessing creditworthiness is more complex. The move from agrarian to industrial society throughout the 19th and 20th century and the advent of mass produced goods was to play a distinct role in the desire for and use of credit; which in turn provided a catalyst to the development of companies specializing in credit checking.

Credit scores are derived from statistical and data-mining techniques. It differs from *credit rating*, because ratings use predictable future information; whereas, credit scoring is primarily concerned with historical information. Here we focus on credit scoring in relation to consumer, rather than business finance, because credit scoring decisions tend to be automated and human decisions seem to be the exception (which is not always the case in business finance). In contrast with its origins, credit scoring based on non-automated human

decisions is treated as highly biased because it depends on the subjective know-how and experience of the credit manager.

III.1.1 How credit scoring works

Historically banks used to rely on the expertise of credit advisors who looked at a combination of accounting and qualitative variables to generate a credit assessment of a particular customer, but in the last few decades most banks have switched to quantitative models.[59] Different financial institutions operate different credit scoring models. For retail customers, a number of 'hard facts' are input into the model, which refer to the information they provide on their current assets and liabilities. Factors such as the amount of credit already accumulated; late payment history; percentage of total credit in use; whether they hold a mortgage account; the age of the applicant; their employment history; length of time at an address all help to reduce risk levels and effect the success of the application. Nevertheless, lenders are keen to stress that lending decisions are not made solely on credit scores, factors such as the type of loan sought, the reason for the loan and the likely profitability of the loan are all influential. If the customer is has existing products with the lender, the type and history of that customer relationship is assessed.[60] Lifestyle information, as represented in Experian demographic profiles, may also be used. The biggest drawback of hard facts is the focus on data from the past.[61] Other critical aspects are the completeness of data, the factual data accuracy and the issue of mistaken identity.

Each of these variables are given a statistical weight and plugged into a model. The most commonly used credit assessment models are: heuristic models (classic rating questionnaires, qualitative systems, expert systems, fuzzy logic systems), statistical models

---

[59] Hayden, Evelyn (2003): *Are Credit Scoring Models Sensitive With Respect to Default Definitions? Evidence* from the Austrian Market, University of Vienna, Department of Business Administration Chair of Banking and Finance, Vienna.

[60] Thonabauer, Günther; Nösslinger, Barbara; Datschetzky, Doris; Kuo, Yi-Der; Tscherteu, Alexander; Hudetz, Thomas; Hauser-Rethaller, Ursula; Buchegger, Peter (2004): *Guidelines on Credit Risk Management – Rating Models and Validation.* Published by: Oesterreichische Nationalbank (OeNB), Financial Market Authority (FMA), Vienna.

[61] Strobl, Gerhard; Hahn, Friedrich (2010): *Lehrgang für Finanzmarktaufseherinnen und -aufseher, Modul 1.07, Einführung Kreditgeschäft.* Aufsichtsakademie der Finanzmarktaufsichtsbehörde und Österreichischen Nationalbank, Skriptum, September/Oktober 2010.

(multivariate discriminant analysis, regression models, artificial neural networks), causal models (option pricing models, cash flow models) and hybrid forms. [62]Heuristic models attempt to incorporate the subjective experience of lenders as well as information pertaining to the customers. Statistical models attempt to verify hypotheses using statistical procedures on an empirical database. The accuracy of fit of any statistical model thus depends heavily on the quality of the empirical data set used in its development. The rating levels which are the outcomes of the process are usually expressed in terms of 'grades' similar to a school grading system. The implications of a bad credit score are a general exclusion from economic participation and in particular, unsuccessful applications for credit, the refusal of further loans and credits, refusal of phone contracts, refusal of purchasing by mail order, a deterioration of payment terms, a deterioration of procurement terms and withdrawal of loyalty cards.

In this case study we examined credit scoring practice in five European countries: Austria, Hungary, Italy, Norway and the UK. We found considerable variation in the importance of credit scoring in these countries' respective financial services industries. We attributed this to national differences in banking practices and the differing importance (and availability) of credit in those historically embedded practices. The main difference between the countries concerns the importance of credit in relation to house purchases, patterns of home ownership more generally and the prevalence of personal debt and credit cards. In Austria, for example, it is more usual to rent a home than to buy it. Small numbers of people are subject to credit scoring and so in general there is low awareness of the practice. In Hungary, there is widespread home ownership and a desire to 'trade up' in the housing market. There is also a strong desire for consumer credit, but it is not widely available[63]. Most citizens are aware of Hungary's 'debtors list' and that information is shared about credit scoring, but debt is seen as shameful in Hungarian culture. Moreover the debtors list has been used maliciously (i.e. individuals names entered erroneously in order to damage their

[62] Thonabauer (2004) op cit.
[63] http://www.euromonitor.com/consumer-lending-in-hungary/report accessed 19th May 2014

livelihood and reputation). In Italy, it is usual for parents or grandparents to buy a house for their children, so credit scoring only applies to people of a certain age. As such, there is low awareness of credit scoring in the general population and banks decisions are trusted by consumers. Consumers associations are weak in terms of their ability to question the actions of banks in relation to their customers. However the Italian tax office is now employing a credit scoring- style system to calculate tax liability, which is far less popular. In Norway, as in the UK, access to consumer credit is the norm. Creditworthiness is a normal part of life in Norway and there is widespread awareness of credit scoring. Consumers are also empowered in relation to credit scoring itself, with a highly transparent system in operation and standard notification of when one is subject to a credit scoring enquiry by a third party. In the UK, home ownership is widespread and it is usual to 'trade up' in the property market, although housing is expensive. Credit cards, consumer finance and personal loans are not only a normal part of life but are seen as essential to getting on in life. Young people are expected to enter into debt to receive higher education. Re-financing and consolidating one's debt is commonplace (although not always recommended). Recent controversy around pay day loans (high interest, short term loans) has arisen because low levels of financial literacy, particularly in the working classes, have resulted in unmanageable debts for some individuals. Debt is not shameful in the UK, it can be something to boast about.

III.1.2 The history of credit scoring

In *Austria* the first organisation to initiate a database which aimed to assess the creditworthiness of customers was the so called 'Creditor Association for the Protection of Claims in Case of Insolvencies' (Creditorenverein zum Schutz der Forderungen bei Insolvenzen). Today, this organization is known as the 'Credit Protection Association' (Kreditschutzverband, KSV 1870).[64] The KSV was founded on April 10th, 1870 in Vienna. In

[64] http://www.ksv.at/KSV/1870/ (accessed 05 Oct. 2013).

their article, Krenn & Zeger (2009)[65] claim that the KSV 1870 was the first such organization in Europe, whereas Knyrim (2008) mentions the German organization 'United Credit Bureaus Bürgen' (Vereinigte Auskunfteien Bürgen) from 1862. Similar Austrian institutions are the 'Creditreform', founded in 1889, or the 'Carinthian Creditor Association' ("Kärntner Kreditorenverein"), established in 1924 and now known as 'Alpine Creditor Association for Credit Protection and Business Economics' (Alpenländischer Kreditorenverband für Kreditschutz und Betriebswirtschaft, AKV).

Over time, the KSV 1870 gradually expanded its services. In 1913, the services 'encashment'/'collection' (Inkasso) and 'information/inquiry' (Auskunft) were added, and in 1955 a judicial representation for claims (gerichtliche Forderungsvertretung) was introduced. In 1964, the KSV finally began gathering information on private persons. The 'small loan cadastre' was established (known today as 'consumer credit registry' (KonsumentenKreditEvidenz/ KKE), the list of unwanted accounting connections (Ungewollte Kontoverbindungen, UKV bzw. Warnliste der Banken, WL) was introduced, and since 1997, the 'goods credit registry' (WarenKreditEvidenz, WKE) has mainly been used for mail order and telecom companies (Krenn & Zeger 2009). The 'goods credit registry' also provides addresses and identity checks as a service for companies. Many of these registers also refer to Deltavista, a company which opened an office in Vienna, Austria in 2000. In 2011, CRIF acquired Delta Vista Switzerland and Austria. CRIF describes itself as a leading provider of credit management solutions in Europe. Its headquarters are located in Bologna, but there is also a branch office in Vienna. Besides a relatively small number of companies with their own data sets (about 5 - 7), a wide range of encashment services, detective agencies and other credit reference services offer economic information (Krenn & Zeger 2009).

In *Hungary* credit scoring has emerged in post-communist times. Commercial banks raised the idea of establishing a central debtor list several times in the early 1990s. However, at

[65]Krenn, Michael; Zeger, Hans G. (2009): *Datenschutzbestimmungen zur "Auskunft über die Kreditwürdigkeit"*, in: Bauer, Lukas; Reimer, Sebastian (Hg.) Handbuch Datenschutzrecht, Wien, facultas.wuv, S. 533-549.

that time there was no commonly agreed opinion on the concept of such a register even inside the financial sector. Banks were not interested in sharing confidential information about their lending policy with their competitors, and the legal framework also did not support the founding of such a credit information system. The confidentiality of banking data was protected by regulation on bank secrets and business secrets, while the autonomy of the natural person (i.e. customers of commercial banks) was guaranteed by their right to informational self-determination. Consequently, a comprehensive legal framework had to be devised, within the limits of the general legal system established after the change of the political system.

The first step towards such a legal framework was to amend the then existing act on financial institutions. The amendment was made in October 1993 and the 'debtors list' was born. This amendment lifted some of the restrictions on forwarding information which constituted a bank secret. According to the new provisions, the provision of the following information, which had previously been confidential to banks, was permissible: information about the person's bank account name (description) and number; general information (containing no details); their solvency (unless their service contract expressly forbids it). Banks could also share information about which customers were in debt with the central credit information system, creating a debtors list. This list was then recirculated to all institutions.

On this legal basis eight leading commercial banks in Hungary established a joint venture called Inter-Bank Information Service Corporation (BISZ), which started to operate the Inter-Bank Debtor and Credit Information System in June 1995. While in Western European countries the central banks established such registries, in Hungary the commercial banks took on this role. Soon after the launch of the registry smaller banks also joined the system, and by 1996 virtually the whole financial loan market entered the Inter-Bank Debtor and Credit Information System. In 1998 the new Banking Act made it obligatory for all financial institutions offering loans to join the system.

However, the 1993 amendment did not allow the registration of natural persons in the registry, because of data protection. At that point only account type and account numbers were shared. At that time financial loans to natural persons were offered predominantly by a single financial institution, the National Savings Bank, which had a monopoly in handling citizens' financial matters before the political changes. In the second half of the 1990s the expansion of demand for credit made it necessary to include provisions regulating the use of credit information on natural persons, too. This finally occurred in 1998 when an amendment of the new CIFE Act made it possible for individual debtors, whose debt exceeded the minimum wage and who were in default for more than 90 days, to be included on the list.

Thus the first period of the Inter-Bank Debtor and Credit Information System – later renamed as Central Credit Information System – had been functioning solely as a "negative" debtor list until 2011. In this period the Inter-Bank Information Service Corp. became a sole-owner institution (owned by the GIRO Clearing House Corp.) in 2003. In 2005 a comprehensive customer protection reform took place, as a result of the high number of customer complaints submitted to the Hungarian Financial Supervisory Authority and the Parliamentary Commissioner for Data Protection and Freedom of Information. The majority of the complaints revealed that the customers had not been sufficiently informed about the existence of the debtor list. The only realised they were on the list when their loan applications were rejected. Furthermore, it was difficult to have access to one's own data in the list and to correct inaccurate data or delete the data if entered unlawfully, furthermore the customers had no efficient legal remedies in matters related to the central debtor list.

In 2002, the Hungarian Banking Association initiated consultation with the government on the introduction of the positive debtor list model. However, the subsequent data protection commissioners had managed to block these attempts to broaden the credit reporting system until 2011. Now, the central credit information system, containing both the negative debtor list and the positive debtor list, has become a major component of credit scoring practice

within banks and other credit institutions. According to the statistical data published by the BISZ Corporation, in 2002 data of credit contracts of 155,000 individuals were stored in the system, while this number has recently reached 4.8 million (in a country of approximately 10 million inhabitants).

Currently, Hungarian financial institutions are obliged to credit check all credit agreements (also financial leasing arrangements) concluded with natural persons, including real estate and car financing. Lenders are not allowed to offer loans to the borrowers solely on the basis of credit risk contributions, they are obliged to check the financial standing of natural person applicants in each credit arrangement procedure. The checks are to be based on the personal or family income of the applicants [Section 3 (1)-(2), Act CLXII of 2009]. The result of these checks is that the individual credit limit for each borrower, defined in the local currency (Hungarian Forint), is the maximum amount they can afford each month. Banks can only provide loans where the monthly payment is within this amount.

In *Italy,* as table III.1 shows (Bofondi, Lotti 2006: 24), the adoption of Credit Scoring techniques by Italian banks started in the late '80s and was increasingly implemented due to the standardized approach to credit risk endorsed by the Basel Capital Accord (2001).

	Any purpose	Consumer	Mortgage	Small business
First adoption	1989	1989	1993	1993
Year				
1993	3	3	1	1
1994	4	4	1	1
1995	5	5	1	1
1996	6	6	1	1
1997	8	8	2	2
1998	13	12	5	5
1999	28	22	19	6
2000	50	37	31	14
2001	60	45	41	21
2002	76	60	54	27
2003	77	61	58	32
% of banks	23.3	18.5	17.6	9.7

Table III.1 Number of Italian Banks adopting credit scoring (cumulative) by year [66]

[66]Bonfondi M., Lotti L., 2006, *Innovation in the Retail Banking Industry: the Diffusion of Credit Scoring,* https://mail.sssup.it/~lotti/Bofondi_Lotti.pdf page 24

Italian banks have been slow to adopt credit scoring in relation to consumer finance, mortgages and small business finance. The main reasons for this include: a) the slow diffusion of technology b) the lack –until a few years ago- of comprehensive credit bureaux and c) the reliance on qualitative/soft information when dealing with customers.[67] Additionally, the large number of small banks, especially in rural areas, discouraged the use of standardized techniques in favour of the informal credit assessment of customers. The adoption of credit scoring significantly increased after 1998 and in early 2000 it started to play a major role within large banking groups.[68] The diffusion is also linked to several changes which occurred in the 90s that boosted the use of credit scoring, namely a noteworthy reduction in the number of banks (from 1,138 in 1990 to 779 in 2003), the privatization of commercial banks, the creation of large banking groups and the implementation of international legal provisions. At the same time, research conducted by the Bank of Italy indicates that only 10% of institutions they surveyed used credit scoring in 2000 while the situation changed completely in 2006 when more than 50% claimed to have adopted it (Banca d'Italia 2010:26).[69] It is also interesting to consider what kinds of information sources are included in scoring systems, one of them being qualitative information both for medium-sized, large and mutual banks (Banca d'Italia 2010: 28).[70] Storing techniques are widely used but "they are still rarely employed to determine interest rates and loan maturities", moreover, when it comes to decisions of whether or not lending to SMEs, credit scoring tools are "decisive" only for 18% of sample and for a third of large banks.[71] When looking at the development of credit scoring within the national context, there are other features to consider which have encouraged the adoption of credit scoring. Banking reorganization - such as decentralization – and the presence of foreign banks have

[67] Ibid, page 6
[68] Banca d'Italia, *Centrale dei Rischi-Foglio informativo*, in Circolare della Banca d'Italia n.139/91, "Centrale dei rischi. Istruzione per gli intermediari partecipanti", http://www.bancaditalia.it/serv_pubblico/elenco-dei-servizi/info_archivi_CR/links/per-approfondire/foglio-informativo-CR.pdf
[69] Ibid, page 26
[70] Ibid, page 28
[71] Ibid, page 29

accelerated competitive pressure in the credit markets and consequently have fostered the need for automated decision making processes. As such, credit scoring is a growing practice in Italy, but main is deployed in relation to mortgages. However the government have developed a system based on credit rating to tackle tax evasion. The controversial *Redditometro* system, which accesses directly the financial records of private citizens via their banks and other institutions with whom they have contracts, to assess their assets and liabilities for tax purposes.

In *Norway* the evolution of credit information services dates back to the mid-19th century. Then, the service was carried out alongside debt collecting. Prior to the establishment of credit scoring agencies, the person seeking credit had to contact banks, suppliers etc. and gather the references needed. Eventually, a central register was needed, and then, the need for credit scoring agencies emerged. Credit information services organisations began to appear at the end of the 19th century. As Norway began to participate in international trade, international branches of these agencies were established. Initially, the credit information service itself required no special qualifications, and there were no particular rules regulating the service.

The emergence of the Norwegian Data Protection framework in the early 1970s was partly driven by the developments in credit scoring. Two committees were appointed by the Parliament, and one of them was named *Kredittopplysningsutvalget* – the Credit Information Committee – because of its strong focus on credit information agencies. This committee was led by a professor of law, Tore Sandvik, and had seven additional members. Four of these were representatives suggested by credit information agencies and credit scoring agencies. There was wide political consensus about the need for data protection legislation, and the debated issues at stake revolved around how to define the limits for the use of the data. The mandate of the committee was to investigate the use of personal data in the private sector. The following year, the second committee, the *Datautvalget* – Data Committee – was formed to carry on the same task for the public sector. The reports of the committees, including

suggestions for new legislation, were released in 1974. The Credit Information Committee proposed general rules for the registration of information in registers, and drafted the guidelines for the licence system. The Data Committee built on this work, and added suggestions about guidelines for a common regulatory authority to be responsible for the license system, and to make sure that the legal provisions were followed. These two suggestions were later translated into a unified act by the Ministry of Justice, and were presented to the government as *Ot prp nr 2* (1977-78) *Om lov om personregistre m.m.* The *Personregisterloven* was adopted on the 9th of June 1978, and implemented 1st of January 1980. Both the right to access her own data (Section §7) and the right to make corrections to her data (Section §8) were included in this act. Section §40 protected the individual against possible economic damage caused by use of incorrect information by credit information agencies, obliging them to replace eventual economic loss of the individual.

A classic example of the workflow of credit scoring is the following: an individual wants to purchase a service including credit, e.g. setting up a cell phone subscription. She signs a contract with her name, national ID number, address etc., agreeing to the relevant terms and conditions. The latter include the possibility to carry on a credit check on the prospective cell phone subscriber. Then, the credit provider (in this case, the phone carrier company) uses the services of one of the licensed companies to obtain the credit score of the individual. No matter the outcome of the credit check, the prospective customer (the data subject) receives a notification by mail or email including the information that the phone carrier company received from the credit scoring agency. If the notice to the credit provider comes with the conclusion that nothing negative is registered on her, or with a score that is deemed appropriate by the credit provider, the cell phone subscription is put into action. Otherwise, the credit is denied (in this case, the mobile phone subscription). If the subscription is denied, or the data subject notes errors in the information that has been provided by the credit scoring agency, she can complain to the same, and, if deemed necessary, to the Datatilsynet.

To date, eleven enterprises hold a credit scoring license from the DPA. In order to get a credit scoring licence as a private company, one must demonstrate that there is an 'objective need' to credit score to the Norwegian DPA. We discuss the legal basis of this in section III.4 of this report. Norske Kredittopplysningsbyråers Forening (NKF) (Norwegian credit scoring agencies union) is an umbrella organisation organizing the major credit scoring agencies. Soliditet Decision, one of the eleven, has performed credit scoring for over a hundred years, and offers a brief description of its main services. When it comes to credit information on individuals, Soliditet Decision uses a database "contain[ing] information about approximately 4.2 million Norwegians".[72] Everyone with taxable income is registered with the credit information agencies. The kinds of information contained in the database are diverse: "basic personal data, Decision Score Person, tax assessment (past three years), estimated gross income, name and address history, business interests, non-payment records and any security furnished voluntarily".

The Decision Score Person is a score representing a meta-analysis of all kinds of data about the person by Soliditet Decision. It synthesizes the overall credit score by ranking individuals according to a predicted risk of default. According to their website:

> Decision Score Person tells you in a simple and user-friendly manner which customers have a high, medium and low risk of default. On the basis of extensive analyses, we have identified the most important variables that best predict the likelihood of a person defaulting on commercial credit (non-payment record or debt collection) during the next 12 months. These variables, by themselves or in combination, decide which zone a person belongs to. In addition to the statistical likelihood of defaulting on commercial credit, we also employ a set of overriding policy rules that may affect the decision to grant credit.[73]

[72] https://www.soliditetd.no/en/products. The total population of Norway reached five million in 2012.
[73] http://www.regjeringen.no/nb/dep/bld/dok/regpubl/prop/2012-2013/prop-195-l-20122013/6/1.html?id=736122

In the *UK* one of the first companies to specialize in credit checking was Equifax and they based their modus operandi on establishing three c's – character, capacity and capital – in verifying the likelihood of repayment. Equifax began in the US in 1899 and established a large database of information on customers – information included: place of employment, marital status, address or memberships to organisations. The databases were in effect files and paper ledgers which included handwritten and typed entries detailing personal information. Up to the 1930s the service was primarily used by mail order companies seeking assurances about their customers before goods were shipped. Other Equifax customers included large department stores or similar organisations selling consumer goods. Throughout the first half of the 20th century the success of such credit checking led to increasing pressure on Equifax and other credit checking companies as the management of the databases and the training of staff skilled in making credit judgements intensified. The pressure on accuracy and time in making decisions helped to create of a numerical scoring system. Scores related to the customers likelihood of repayment; the scores are still in use today and provide a three digit score ranging from 100 to 999 – the higher the number the more attractive the customer to the lender. An advantage the scores provided was to reduce prejudice, bias or personal opinion due to for example race, religion, sex, marital status. Toward the second-half of the 20th century computerization then took credit checking to another level. In the 1960s British financial services organisations began to employ credit scoring agencies to insure their products. Fuelled mostly by the advent and success of the credit card; financial organisations were progressively faced with the task of verifying their customer's capabilities of repayment and the customers current level of debt.

Any financial institution who is lending money employs Credit Reference Agencies to provide credit scores. There are 3 main agencies in the UK, Experian, Equifax and CallCredit. Credit Reference Agencies check applicant's information against databases such as, electoral rolls, court records and fraud data – verifying if fraud has been committed by the applicant or if their name has been used by other to do so. (In addition, lenders use anti-fraud agencies; for

example, *National Hunter* checks previous applications made by the applicant and verifies if any information differs from the earlier applications). Credit Reference Agencies also search information on addresses and 'linked to' data - records of previous searches made by lenders or organisations in relation to the applicant's name, address and previous addresses. The range and scope of information available to Credit Reference Agencies is increasing, for example, energy suppliers British Gas, BT and Scottish Power now share information on defaults or missed payments with Experian. If requested by an individual, agencies must provide a 'Statutory Credit Report' detailing the information used to calculate a score, there is usually a small fee (£2) for this service.

III.2 Stakeholders in Credit Scoring

In a manner similar to that adopted in section II.2, figure III.1 below depicts the core and peripheral stakeholders in credit scoring. The Core stakeholders are watched and watching entities and the stakeholders represented are an amalgamation of the five country case studies which were conducted. The Watched are those who are being credit scored, who, for the purposes of this report, are individual consumers, other private individuals being scored and private businesses. We acknowledge that credit scoring also takes place on a very large scale, with entire countries being afforded a credit rating. Those who use credit scoring therefore vary from suppliers of consumer goods and consumer finance to private landlords and other individuals with an interest in the creditworthiness of their fellows. Peripheral stakeholders are those who have an interest in either the proliferation of credit scoring, such as central banks, infrastructure vendors and those with an interest in economic growth and sound business practice, to privacy activists, consumer protection organizations and data protection authorities who govern and mitigate harms associated with Credit scoring.

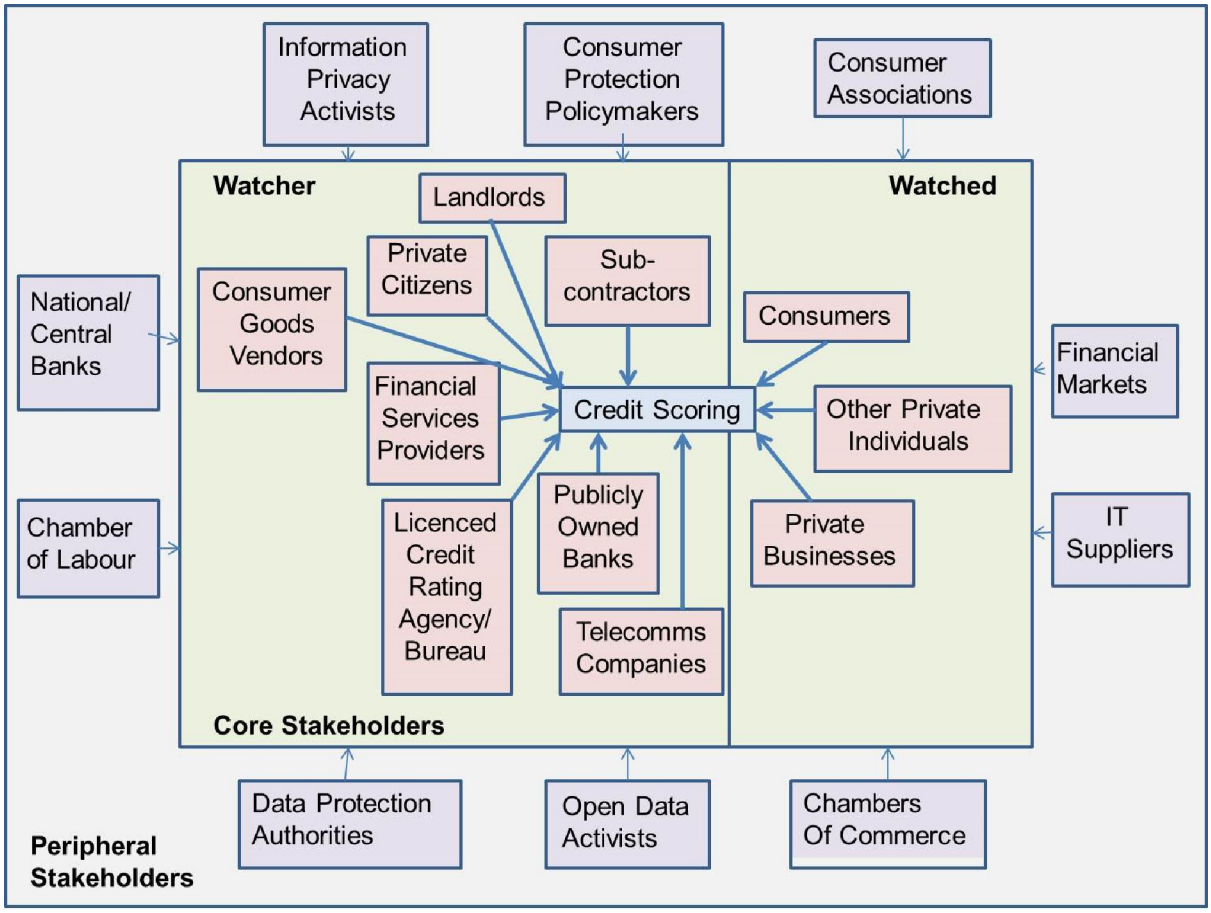


Figure III.1 Stakeholders in Credit Scoring

III.3 Harms and Controversies arising from Credit Scoring

Just as ANPR functions to *prevent* harms, so does Credit Scoring. Accurately assessing the creditworthiness of an individual or a business when they apply for credit protects the interests of both the financial institution and the individual. The financial institution can be assured that the money it lends will be repaid and the individual will know that they can afford to service their debts. Furthermore, the availability of credit to an individual can, when controlled, afford economic opportunity and prosperity. At the level of the economy, it can ensure that businesses thrive and economic growth occurs. Credit scoring is itself a strategy to build resilience, because of the role that it plays in enhancing social and economic stability. Indeed, in three of the countries we studied credit scoring was not perceived as an issue which related to data protection, privacy and surveillance. It was a taken for granted element of the consumer-finance system.

However, credit scoring can create harms. In Work Package 6 of this project, it was reported that credit scoring had a significant role to play in precipitating the global financial crisis of 2008. Poor estimations of credit risk in the sub-prime mortgage market and the hedging of these risks by creating hybrid investment products called 'asset backed securities' underpinned global financial collapse. As sub-prime customers defaulted on their mortgages, asset backed securities became worthless and the subsequent financial collapse had profound consequences for the rest of the world. With more accurate credit-risk assessment, this situation maybe would not have occurred.

More generally, we use the concept of social sorting to discuss the issue of harm in relation to credit scoring. Credit scoring is a social sorting technology in that it electronically sorts through statistical populations and, with the application of an algorithm, defines who is to be afforded certain opportunities over others.[74] These decisions are then applied to embodied individuals and have an impact on their future prospects. Such processes have what Oscar Gandy called 'cumulative disadvantages'.[75] To have a bad outcome in one social sorting process, such as credit scoring, can lead to disadvantages in other areas as opportunities are denied and one's 'bad record' catches up with them – discussed subsequently in the III.3.4. The enabling power of computerization to collect and analyse mass amounts of data was first questioned in the 1970s. Pressing concerns included the possible detrimental effects on personal security and inequality. Throughout this time, and beyond, writers such as Alan Westin challenged computer technologies and their impacts on privacy; his concerns related to the amount and type of information credit scoring companies held on clients.[76] Especially questionably was information that did not have any relevance to credit, for example, marriage status. Whereas in the 1980s sexual orientation had a divisive impact on credit scoring due to AIDs and the risks of exposure for certain populations.

---

[74] Lyon, D. (Ed.). (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Routledge.
[75] Gandy, O. H. (2012). *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Ashgate Publishing, Ltd..
[76] Westin, A. F., & Baker, M. A. (1974). Databanks in a Free Society: Computers. *Record-Keeping and Privacy'Quadrangle*.

Therefore, a discussion of the harms associated with credit scoring begins with questions about the consequences of inaccurate credit scoring decisions but ends with a discussion of distributive justice. We have observed issues with maladministration, the misuse of credit scoring, its role in the irresponsible provision of credit and questions arose over the transparency of credit scoring practices in some of the countries we have studied. In resilience terminology we classify these as 'stresses'. A theme which underpins the following paragraphs is citizens' lack of general awareness of and access to information about credit scoring and the citizens' knowledge of their rights concerning access to data gathered in the credit scoring process, although this is covered in more depth in section III.4 which addresses citizen engagement with credit scoring.

III.3.1 Maladministration

Across the cases we have found a number of examples of erroneous references to individuals on credit scoring databases. In these examples, negative consequences for the individuals had resulted in legal action because of the financial stigmatisation which resulted. These cases also serve to highlight the opacity which is endemic in the data sharing and data processing surrounding credit scoring.

In *Hungary* we found evidence from case law that the central debtors list had been challenged on 32 separate occasions since the legislation was established in the early 1990s. In the vast majority of the cases the plaintiffs had sued financial institutions for wrongly entering them on the debtors' list and had applied to the courts to have their credit records deleted. The majority of the lawsuits found in favour of the banks, because no violation of law concerning the operation of the list was established. The harm caused by the debtor's list is thus not acknowledged in Hungary. Nevertheless, 9 of the 32 cases were filed as a libel case. This means that several plaintiffs argued that registration without legal basis in the Central Credit Information System was defamatory.

For example, a married couple sued the OTP Bank (the biggest commercial bank, which had been operating before the change of the political system as a monopolistic, state-owned commercial bank in Hungary) for a hundred million Forints (about three hundred thousand euros) in compensation because the bank registered them on the blacklist of debtors. The couple lost the government subsidy on their home loan and all other opportunities of getting loans because they were registered on the blacklist. Although the bank later acknowledged maladministration, this did not help the couple since OTP Bank had already forwarded their data to the central debtors list and would not remove it.[77]

In another article the economic weekly reported on consequences of being erroneously registered on the debtors' list.[78] In one case Postabank miscalculated a customer's repayment amount, and while the customer, in good faith, was paying the original instalments as stipulated in the contract, the difference between the original and the wrongly calculated debt repayment reached the maximum level defined by the law. As such the bank registered the debtor on the list. Later the bank admitted its error and deleted the debtor from the list. Another aggrieved party was registered on the list because of a debt of 28 thousand Forints (less than 100 euro), again because of maladministration. In 2004 about hundred customers turned to the Financial Supervisory Authority, either because their names were registered on the list unlawfully, or because they found the consequences of being on the blacklist disproportionately punitive.

While these complainants were notified about their registration on the debtor's list and so were able to complain, a national daily published an article about the blacklist victims who did not know about their registration because – according to the legal provisions in force at that time – they were not notified about it.[79] The victims complained that it was a very

[77]Agnes Gyenis, "Az a fekete folt" [That black spot] *HVG* 2007/14, 07 April, pp. 107-108.
[78] Emilia Papp, "Eros lista" [Hot list], *HVG* 2006/05, 04 February, pp. 92-93.
[79] It should be noted that in 2006 the law regulating the database of bad debtors became more customer-friendly: for example, the bank shall notify the debtor thirty days in advance of registering

complicated and expensive process to retrieve data about the list. Although the banks admitted their maladministration and removed the customer concerned from the list, they were not awarded any compensation.

Interestingly, in a newspaper article published in *Norway* in 2011, which is operates a completely different credit scoring system to that of Hungary, 55% of respondents to a survey alleged that they had been wrongly credit scored.[80] In the Norwegian context it was the consequences of this erroneous credit scoring, not the credit scoring process itself, which was criticised.

III.3.2 Misuse

Research in this work package also uncovered instances where credit scoring had been deliberately misused by financial institutions and their employees.

In *Austria,* in October 2013, a total of 14 people - bailiffs, court clerks and office workers in several district courts - illegally sold the personal data of those involved in court cases to banks and telecom providers allegedly to augment the information upon which the banks based their credit scoring practices. From 2002 to 2010 execution data from nearly 40,000 legal and 92,000 private persons have been collected and resold with a total profit of about 300,000 Euros. The judicial officers were finally found guilty of abusing their authority and breaching official secrecy. They were sentenced to conditional imprisonment of between six to 24 months. Some of the court clerks barely showed any remorse in front of the judge.[81]

The biggest national daily in *Hungary*, *Népszabadság* – quoting the communiqué of the national news agency – reported on the investigation of the Data Protection Commissioner

him on the bad debtors list, and one request per year for the debtor's own data shall be free of charge.

[80] http://www.dinside.no/875910/kredittvurderes-uten-grunn

[81] DiePresse.com (09.10.2013): Gerichtsvollzieher verkauften Justizdaten: "Na und ...?", http://diepresse.com/home/panorama/oesterreich/1462796/Interne-Justizdaten-verkauft_Na-und- (accessed 10 Nov. 2013).

at Citibank. It was found that Citibank had demanded that the personal identification, the tax identification and the social security cards of customers be photocopied and kept on file. The bank justified this action by suggesting that it was a measure to counter-fraud risk, and consequently rejected the credit applications of those who objected to this practice. According to the Commissioner, the bank had retained – for six months - the personal data of even those customers whose applications had been rejected. They argued that it needed these data for preparing internal statistics in order to develop the bank's products. The Commissioner requested access to the credit scoring regulation of Citibank but the bank unlawfully refused the Commissioner's demand on grounds of business secrecy.

It was *Népszabadság* again, which reported about a case in which a student did not get a student loan because he had not consented to the forwarding of his data to a specific bank – Postabank – in order to open an account for him there. The irony of the case was that although the student did not get the loan, his data were forwarded and an account had been opened in his name in Postabank. The spokesman of the Student Loan Center – supposedly as a consequence of adverse publicity in the media – apologized for mistakenly opening the account.

Misuse of credit scoring is a most prominent controversy in *Norway*, particularly in situations which are not covered by legislation. The main issue is that it is available to those organizations who have demonstrated an 'objective need' to credit score. Contraversies therefore arise over situations in which an objective need is difficult to establish. The main problem concerns rental brokers' access to credit scoring for prospective tenants. In 2009, the market leader in home rental real estate, *Utleiemegleren*, was initially refused a credit scoring licence. The board suggested that they should be capable of handling the financial risk and did not need to perform additional checks on their tenants. They filed a complaint against the decision and the refusal was later reversed. The rationale behind the decision was because the company's had a large market share and because it was an agency, (it did not own the properties it rented out) it was effectively credit scoring on behalf of the private

individuals who were renting out their apartments and houses through Utleiemegleren. It was therefore protecting them from economic risk. If *Utleiemegleren* had been a professional rental broker who owned properties and rented them out, the decision would be different based on the fact that the economic risk would be considered normal business practice, and credit scoring would be illegal.

However this case does not seem to be the final statement on the matter. Other smaller rental brokers have had their credit scoring declared illegal and unnecessary for the same reasons that *Utleiemegleren* did in the first place: That they should absorb the credit risk as part of their business practice. This has prompted brokers to introduce a credit element to rental agreements, so that they *must* credit check. Hence they are changing their business practices so that credit scoring is rendered necessary and legal, so that they can get further risk management benefits of credit scoring.

As well as business organizations bending the rules, private individuals have also been exploiting the credit scoring system in Norway, attempting to use it for personal advantage. For example, there have been instances of credit bureaux employees scoring others for dating or relationship purposes, to influence divorce settlements in relation to the sharing of finances and costs, or in cases of child custody – to prove that they are eligible to take care of a child. The misuse of credit information for such purposes is, according to an officer in Bisnode, "on the verge of being idiotic", since every employee who has access to the search functions in the system has to log in with their personal identification.[82] DnB Nord states that such abuses are considered a reason to fire the responsible employee.[83]

Credit scoring of potential job applicants is another area of misuse. In this case, it is unclear as to whether or not this is an acceptable practice as there is not always an "objective need" for credit scoring here either. The DPA states that the rules for credit scoring a job applicant are very strict, and they list three criteria. First, the applicant has to have applied for a very

[82] Cf. http://www.nettavisen.no/okonomi/privat/article2633566.ece
[83] ibid

senior position in the hiring organization. Second, the position has to include financial management. Third, credit scoring can only take place in the final stages of the recruitment process. However, there seems to be no clear mechanism to ensure that these rules are not transgressed. This particular statement was given in relation to a case where professional chauffeurs of long-distance transportation protested against a company credit scoring, by default, all job applicants.[84] The rationale of the systematic credit scoring was based solely on the fact that prospective employees were to handle money, and thus their 'financial morality' had to be checked. The DPA concluded that this particular practise did not fall under the criteria listed, and stated that even if the job applicants had consented to the credit scoring, the practice would still not be considered acceptable.

For the last category of controversies, the emerging issue in the media includes identity thefts leading to unwarranted credit checks. When searching online for media coverage on credit scoring in Norway, a substantial amount of hits concern identity theft. Many cases revolve around criminals obtaining information about the subject's personal data, and making credit purchases, leading to unwarranted credit checks of the identity theft victim. For example, one case included a credit card being stolen from a mailbox, leading to 42 different new phone subscriptions being made in the victim's name, an action requiring the phone companies to perform a credit check.

Following the emergence of these various misuses of credit scoring, the license system was reviewed between 2009 and 2011. The new licence was a result of collaboration with the credit scoring companies, and followed a number of cases from *Personvernnemnda* and the DPA. Among the reasons for the revision was that the potential user of the credit scoring system to bully individuals. Another reason was that the parameters used by the credit scoring agencies were somewhat dubious. In an extremely enlightened moment, the DPA realised that parameters such as age, sex and address can lower a person's credit score

[84] The result in this particular case was that chauffeurs of long distance-transport, did not fall under these criteria. Cf. http://www.transportarbeider.no/kunder/ntf/cms.nsf/($All)/747B6854916FF21DC12578A000371465?OpenDocument

even if they had not had one record of bad payment. The new licence was official since 1st of April 2012. Some revisions were new sources of complaint, i.e. *Norske Kredittopplysningsbyråers Forening* complained about the omission of address history as a parameter. The revision also established a common register for complaints against credit scoring, and that a standard response letter be created in the instance of a complaint. Other that were debated concerned the use of the number of previously performed credit scores as a parameter, property ownership, and information about invoices settled prior to due date.

III.3.3 Transparency and the rule of law

While the Norwegian authorities have been sensitive to the formulation of credit scoring procedures, this is not the case in Austria, Hungary and Italy. As we have already suggested credit scoring in those countries is intransparent and financial institutions have a disproportionate say in how the systems are run. Credit scoring in these contexts serves to concentrate and centralize power in the hands of financial institutions. In these countries there is simply no debate surrounding the rights, privacy or surveillance based implications of credit scoring, in a way which will mobilise existing (for example) data protection legislation to protect individual citizens. Neither citizens nor financial institutions – in other words, neither data subjects, nor data controllers – regard the collection, analysing and use of personal data in connection with credit scoring as a separate phenomenon, or a practice which may restrict citizens' fundamental rights or concern their human dignity. Consequently, credit scoring in general is not understood as a form of surveillance, rather as a set of technical measures involving the processing of certain personal data. Therefore the justifiability, finality and proportionality of data processing are almost never contested by the debtors.

In *Italy*, there is evidence that institutions simply ignore subject access requests for credit scoring data. In one example, a citizen who attempted to obtain a loan from a financial institute (Compass S.p.A.) discovered that he had a negative rating in the Credit Bureau

(Experian Information Service S.p.A.) database, due to previous insolvency. The customer submitted a data access request to Compass S.p.A. as he wanted to know the details of his credit profile, but the company did not respond. In light of this, the citizen brought Compass S.p.A. to court claiming his data access right. The case arrived at the Supreme Civil Court (i.e. *Corte di Cassazione Civile*), which ruled that the data controller in the company was obliged to answer the data access request within 15 days. Furthermore the complex data sources that make up credit scores in Italy can cause problems when data becomes outdated and inaccurate. On 14th May 2013, a citizen appealed to the Data Protection Authority, as she wanted to remove, via Credit Bureau CRIF S.p.A., two real estate liens recorded in the Public Registers on 16 September 1997 and 23 March 1998 respectively. The liens were already settled but had remained on record. However they hampered her access in obtaining credit. CRIF made the excuse that the situation had arisen because their database was supplied by the "Tribunals Information and Real Estate Registers" they had no control over the content. Opaque procedures have thus resulted in an infringement of rights which then require official intervention in order to remedy any harms.

In contrast to commercial credit scoring, government use of credit scoring techniques to assess tax liability has caused an outcry and has prompted debates which invoke surveillant images of 'big brother'. Debate has raged at various levels, from the judiciary to the mass media and have covered the following issues:

1. the potential infringement of the fiduciary duty, where a bank is bound over to respect the privacy and confidentiality of its clients' financial arrangements
2. the potential infringement of the citizens' privacy rights and the related Constitutional principles (among which are the freedom principle, the private property right, etc.)
3. the lack of transparency in its application (the only clear information from the Revenue Agency -*Agenzia delle Entrate*- has been that the *Redditometro* system has a retroactive effect, as the fiscal monitoring of the citizens begins from the year 2009)

4. the defence procedure. i.e. what happens once a citizen is invited to give detailed explanations about expenses or income sources belonging to his/her inheritance (for instance, financial investments, investments in the real estate market and, even, a simple purchase of a new car, under certain conditions)

From the moment the *Redditometro* was enforced, 35.000 letters of inspection have been sent to citizens. The Data Protection Authority was slow to react, and in the breach citizens have brought the Revenue Agency to both fiscal commissions and judicial courts. The majority of judicial rulings on this issue are in favour of citizens' rights. For example an ordinary magistrate (Tribunal of Naples) claimed that the *Redditometro* system is "*operating outside the constitutional and European legitimacy*", as the Revenue Agency does not have "*the power to gather all the personal and sensitive data of an individual and his/her family*". Besides, the judge drew attention to the infringement of arts. 2 and 3 of the Italian Constitution and to the Charter of Fundamental Rights of the European Union. Therefore, according to the Judge of the Naples Tribunal this fiscal control system "*is not only illegitimate, but radically null and void"*, because it *"infringes upon the legal principles of equality, reasonableness, proportionality*".[85]

Therefore, it seems that the *Redditometro* has been assessed, both by citizens and judicial authorities, as a tool which might infringe fundamental rights. The system has been perceived as highly invasive and has generated what we might call "resilient attitudes" from citizens and judges alike. Resilience has emerged more in relation to this tool than to the practice of credit scoring for reasons that are difficult to grasp and go beyond the aim of the case study. However, one might speculate that the *Redditometro* was described in detail in the media and was hence more transparent in comparison to credit scoring.

[85] Greco A. M., *I giudici arrestano le tasse «Il redditometro è nullo»*, in Il Giornale, 27 September 2013 , p. 10

This concentration of power has also revived neoliberal discourses of responsibilisation in the *Norwegian* context. These neoliberal ideas are being expressed by the major credit scoring agencies, such as DNB Nord and Dun & Bradstreet, who are challenged by the wide ranging definition of 'objective need' described earlier. According to Dun & Bradstreet, the responsibility for ensuring that the credit check is valid lies with the clients buying their services rather than with the agencies themselves. This means that the responsibility for interpreting the legislation shifts from the credit scoring agencies and to the large number of clients performing credit-based services. The DPA has few ways of sanctioning the companies, other than letting them know what is considered the right practice. Credit checks can be performed in relation to very small amounts of money, making the possible scope of the practice quite wide. The DPA reports to have handled cases where sums as low as 200 NOK (approximately €23) have been considered as a sufficient risk for the credit providers, and hereby approved as an "objective need" for credit scoring. Paired with the lack of obligation to check requests upon disclosure and the low limiting effect of the definition of "objective need", the responsibility and accountability of credit scoring is mostly shifted from the credit scoring agencies to their clients.

III.3.4 Use of credit scoring in cases of irresponsible lending

The final harm is the use of credit scoring to approve financial services products targeted at the vulnerable and financially illiterate. This is the issue of payday loans. The practice of payday loans has caused huge controversy in the *UK*, because it is seen to target the financially vulnerable, as well as charging extortionate rates of interest. Traditionally, payday loans are purchased by those who do not have access to more established means of credit purchase, such as through banks. Often customers have exhausted other opportunities of gaining credit due to historical financial difficulty or being on low incomes or government support. Pay-day loans are a well-established form of lending, however in more recent times the market has grown substantially and as a result is now a rather lucrative business in the UK. A major contribution to the growth is the ease of access now provided by companies

online; effectively loans can be secured from home, via a smart phone, within minutes. In some instances there is no need to speak to an operative to secure the loan as credit checks and authorisation is automated.

UK MPs have been vocal in calling for a cap on the charges allowed, have been instrumental in calling for tighter regulation on the industry and in November 2013 the Business, Innovation and Skills Committee questioned representative from pay-day loan organizations, as well as consumer advice bodies.[86] The session explored issues raised in a 2012 report on UK Debt Management and was intended to inform how further regulatory measures would be implemented in 2014. Indeed, some political commentators have called for this type of loan to be rebranded as 'high-cost short-term credit'. In addition, what has also been highlighted is the hidden implications of taking out a pay-day loan, as the act affects credit scores with some mortgage providers. These consequences it has been argued should be highlighted by the pay-day loan organisations. Moreover, much of the concerns raised by MPs and the public have focused on the light touch regulation that has been adapted by the Office of Fair Trading and indeed, by the Financial Service Authority. Much of the frustration in this regard emanates for the controls and checks that failed to stop the lending and borrowing by UK banks in the lead-up to the financial crisis of 2007.

As a result of the Committee and the publicity generated, as well as mounting public and media pressure the industry is 'fighting back' and has launched a charm offensive of sorts. Included has been a commissioned 30 minute film – the film is a sentimental look at the 'real Wonga stories' of 12 customers. Each story begins with a customer's voiceover stating 'I love to..', the uncomplicated message of the film is Wonga's role in helping customers in their quest for betterment. Accompanying this promotional contrivance, the profile of Niall Wass, the chief executive of Wonga, has also been heightened. Since November 2013 he has appeared on number of high profile news programmes such as BBC Newsnight.[87] On

[86] http://www.bbc.co.uk/news/business-24814037
[87] http://www.bbc.co.uk/news/business-24814037

these he has sought to vindicate the processes and motives of his organisation. He has stated, customers are happy with the services provided and that the interest rates Wonga provide are competitive. Typically, he states, Wonga's interest rate of 1% per day and Wonga's lending terms are clearly explained to all customers. One of the leading complaints toward the company is that due to the online and automated nature of the company checks and verifications are easily circumvented. Regular examples include customers fraudulently stating they are in employment. Rarely does it appear these discrepancies picked by the online decision technology. In addition, Wonga and other loan companies have been adamant in their claims that they are not 'Loan sharks' (a term used for unlicensed lenders, who often use unscrupulous means to gather repayments from extremely high interest loans). Wonga are unequivocal that they never use threatening behaviour toward their customers; however some media reports suggest customers do face daily phone calls if payments are late; this has been described as 'harassment' by some customers.

III.3.4 Summary

While credit scoring promotes financial opportunity and enables both individuals and institutions to manage financial risk we have observed that the system is open to abuse. Credit scoring invests an enormous amount of power in the hands of financial institutions and credit scoring agencies. As a social sorting technique, credit scoring enables this power to be applied over the future of individuals as well as the economy as a whole. The functioning of that power varied across the cases, particularly in terms of the following:

- the accuracy with which it was wielded
- the responsibility with which it was wielded and the extent to which it was used as a tool to exploit the vulnerable
- the accountability of powerful financial institutions and credit scoring agencies to regulators and the judiciary
- the transparency of credit scoring to the public

- the power of the regulators in relation to credit scoring, particularly in terms of the sanctions they can impose.

We now look at this issue in more detail by examining different democratic encounters with credit scoring.

III.4 Democratic Encounters with Credit Scoring

In this section we examine how credit scoring is governed, the extent to which its stakeholders participate and co-determine the practice as well as the extent to which individuals engage with it. We find that governance is strong and centralised in all countries, but there is differential intersection between financial governance and data protection laws. The participation of peripheral stakeholders in the practice is practically non-existent, but there is clear co-operation between watchers to maximise the sharing of relevant data on customers. Public engagement with credit scoring varies across the cases. In the UK and Norway, there is a high level of public engagement with credit scoring, but for very different reasons. However in Austria, Italy and Hungary it is more secretive and less transparent to the public.

III.4.1 Governance

At a European Level, the most important regulation within which credit scoring is encompassed comes from the 'Basel Committee on Banking Supervision' (BCBS). The so-called 'Basel Accord' (initially referred to as Basel I) is a credit risk framework introduced in 1988 by which the Basel Committee on Banking Supervision which defined capital standards for international banks in member countries (G-10 countries). This committee does not have any legislative enforcement capability, but it can propose the main rules and directives that each Country should adopt and adapt within its specific legal system The objective of the Basel Accord was to limit the banks' business risks by banking supervision and strengthen the financial system overall. In order to meet the requirements of ongoing developments in

banking, the Basel Committee began revising these requirements in 1999, and the new capital accord ('Basel II') came into effect in 2007. Basel II introduced a “rating system” to enable the banks e to limit the risk of the credit market. Paradoxically, the system was aimed at strengthening the *resilience* of the banking sector. This agreement was enforced on 1st January 2008.[88]

The requirements of the latest accord (Basel III) serve to increase the stability of the international financial system by introducing more risk-sensitive minimum capital charges for debt exposure, expressly accounting for operational risks, reinforcing the role of financial market supervision and increasing market transparency. In a parallel process, the European Union (EU) developed the Capital Requirements Directive (CRD), which pursues the same objectives and applies to all banks and investment firms in the EU once it has been implemented in the national legislation of Member States. Basel III shall come into force in 2014 (see Deliverable 6.1).

As such, several pan-European laws, directives and regulations govern credit scoring:

1. Basel I + II + III (Basel Committee on Banking Supervision – BCBS)

European Directives

2. Directive 2008/48/EC on credit agreements for consumers
4. Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions (cf. Article 8)
5. Directive 2006/49/EC on the capital adequacy of investment firms and credit institutions
6. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (cf. Article 15 - Automated Individual Decisions)

[88] Orsini C., *Da Basilea 1 a Basilea 3*, Arcadia Consulting Srl, Bologna, 2010, www.arcadiafinance.eu

In particular the EU Directive 95/46/EC "*on the protection of individuals with regards to the processing of personal data and on the free movement of such data*" is the basis of any national legal provision for personal data retention, including the Italian legal framework on the Credit Scoring practice specifically referring to sensitive data gathering and management (*ad hoc* databases) by the different financial stakeholders involved in this procedure.

We also note that credit scoring is implicated in the European Wide regulations on the prevention of Money Laundering and Terrorist finance, first outlined in the Vienna Convention of 1988 and enshrined in the Third Anti Money Laundering directive, to be revised and updated in 2014.

At country level, a variety of additional regulations are in force. In *Austria*, there has been a gradual refinement of rating and scoring methods and an approximation of credit assessment applications for the retail market and private persons. Furthermore, it can be said that there is increasing transparency and regulation, even though these developments have not necessarily created a balanced power relation between credit scoring agencies and the concerned individuals.

The Austrian National Bank (OeNB) and the Financial Market Authority (FMA) require banks to maintain certain standards in the granting of loans. This is assessed by statutory auditing processes. The auditor must obtain an overview of the structure of the bank's internal control system and the adequacy of the relevant control measures for rating systems. Audit priorities include the development of the rating methodology, its on-going validation. The results it yields in terms of the distribution of ratings across the customer base is also relevant. These standards and regulations, however, are less focused on data protection and ethical criteria than on the solvency of the bank and the stability of the financial market. Knowing as much as possible about the customer is good business practice, sanctioned by regulation (see also 'know your customer' - policy; money laundering/terrorism financing). The economic stability of the financial market is therefore in conflict with individual rights and the confidentiality of personal data. Furthermore as a result of mergers, name changes,

relocation of offices, cooperation and joint ventures as well as the sale of databases, the market is cluttered and the stakeholders repeatedly change. In addition, by transferring their data stocks to companies based in foreign countries like Germany or Slovakia, the Austrian data protection regulations can be circumvented.[89]

Numerous Austrian national laws delimit where, when and how credit scoring can be used, as follows:

1. Banking Act (Bankwesengesetz, BWG) cf.§ 39;
2. Trade Regulation (Gewerbeordnung 1994, GewO), cf. § 152;
3. Consumer Credit Act (Verbraucherkreditgesetz, VKrG)
4. Data Protection Act (Datenschutzgesetz 2000, DSG), cf. § 49;
5. Gambling Act (Glücksspielgesetz, GSpG)
6. Loan and Credit Law Amendment Act (Darlehens- und Kreditrechts-Änderungsgesetz, DaKRÄG)
7. Solvency Regulation (Solvabilitätsverordnung, SolvaV)

Use of credit rating is not only possible - see for example § 152 Trade Regulation (GewO) 1994 – , but even explicitly required in some cases, for instance with regard to gambling (see § 25 Gambling Act). The failure to obtain required background information on creditworthiness of customers may result in legal consequences.[90] The Austrian Data Protection Act says that consumers have the right to request a copy of all the data held on them by Credit Bureau (CRIF/KSV1870). If one applies for credit and if this application is unsuccessful it is then not possible access any of the data upon which the decision was made. The Data Protection Authority is powerless in this respect.

[89] Krenn & Zeger 2009, op cit
[90] Knyrim, Rainer (2008): *Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?;* in: ecolex Zeitschrift für Wirtschaftsrecht, S. 1060-1062.

The regulation and governance of credit scoring in *Hungary* has been extensive. Until the global financial crisis in the early 1990s, the regulation of the activities of financial institutions was rather liberal, with no significant regulatory restrictions on credit scoring. The Parliament enacted a general provision in 1993 stating that financial institutions providing loans were obliged to obtain information about the credit standing of the borrowers and their guarantors. Even the comprehensive legal reform of the financial sector, which took place in 1996, did not introduce new provisions regarding the checks on the borrowers' financial status.

Act CXII of 1996 on Credit Institutions and Financial Enterprises (hereinafter: CIFE Act), which is the most important act in the area of loans and which is applicable to all financial services provided in Hungary, provided only for certain general rules on credit rating as part of the prescriptions concerning the requirements of prudent operation of credit institutions. For almost two decades scoring attributes were regulated only in the internal regulations of financial institutions, the preparation of which are stipulated in the CIFE Act: "Financial institutions (…) must adopt internal rules and regulations, subject to approval by the board of directors, to provide sufficient facilities to establish the substantiality and transparency of placements and exposures as well as to control the assessment of risks and to mitigate them".[91] Other general provisions include that "Prior to deciding on a placement, the credit institution must ascertain the existence, value and enforceability of the necessary collaterals and securities. The documents substantiating such decision must be attached to the contract for the deal." [Section 78 of CIFE Act] Consequently, the credit scoring practices has been developed by the commercial banks individually, constituting sensitive business secrets.

Although the present legal regulation still provides significant room for self-regulation, the laws enacted as a reaction to the global financial crisis restricted the independence of financial institutions in the area of credit rating. The most significant regulatory change regarding credit scoring was the Act CLXII of 2009 on retail lending, and its implementing

[91] Act CXII of 1996 on Credit Institutions and Financial, Section 77 CIFE Act

Government Decree No. 361/2009 (XII. 30). The aim of the Act was to achieve profound changes in the practice of retail lending with a special focus on consumer protection in order to meet the expectations of the European Union declared in the Consumer Credit Directive 2008/48/EC. These statutes contain specific rules on credit rating for ensuring the correct and reliable information on the consumers.

The latest law relating to the Central Credit Information System (CCIS) in Hungary was passed in October 2011. This has re-regulated and expanded the scope of the CCIS. The project was managed by the Hungarian Banking Association, the BISZ Corporation and financial stakeholders. The law-makers introduced the mandatory registration of positive credit data on natural persons. However, while no statement of consent of data subjects is required for access to negative information, registration in the positive debtor list makes access by financial institutions dependent on the opt-in based consent of the customer concerned. Customers should give such consent in each case, otherwise their bank will only receive information on past events of credit default and fraud, without any positive credit data, for the purpose of assessing credit applications. Banks decide the criteria they are to use in evaluating the creditworthiness of a potential customer.

In Hungary Credit Scoring is regulated by the Hungarian Financial Services Authority and the Parliamentary Commissioner for Data Protection and Freedom of Information. Earlier on in this report we noted that a number of complaints had been filed about the CCIS to these authorities, particularly to the Data Protection Commissioner. In the 1990s, the commissioner received complaints about the necessity and proportionality of broad financial data collection by financial institutions. In the 2000s, complaints increased exponentially, indicating increasing public sensitivity to the fate of their financial data and the principle of finality arose: i.e. that data should be collected for a specific time only and the data collected would not be in excess of what was required. This was particularly the case in relation to the banks retention of data about rejected clients on file without authorization by law, for product development purposes. In this matter the President of the Financial Supervisory Authority

shared the Commissioner's standpoint and proclaimed that keeping and using such data ran counter to the principle of finality enshrined in the data protection act.

The complaints received by the Commissioner, however, have partly helped to change banking practices around credit scoring. By 2005 the 40 percent of the cases regarding the data processing practices of financial service providers contained complaints against the operation of the central credit information system. However, after new legal provisions regulating the system, making the operation of the system more user-friendly, this number dropped to 1-2 percent, and the complaints submitted proved to be unfounded. This shift clearly shows the interdependence of the legal regulation and the Commissioner's quasi case law. However by the end of 2010 debt collection was still the area of the banking industry most criticized by citizens.

In *Italy*, the legislative framework focuses its attention on the Credit Scoring procedure which has been the subject of specific intervention by the DPA. It has enforced detailed rules for the collection and management of consumers' data. The "Data Protection Code" (DP Code) has devoted an *ad hoc* part of the Code to consumer finance, focusing attention on the data retention and management in this context. The DP Code, Part II – "*Dispositions referring to specific sectors*", Title IX – "*Bank, financial and insurance systems*", Capo I – "*Information systems*" describes the set of rules addressed to data collected in the financial and insurance systems for different purposes and its protection:

- Art. 117 – "*Reliability and punctuality in payments*"
- Art. 118 – "*Commercial information*"
- Art. 119 – "*Data referring to the debtor's position*"
- Art. 120 – "*Accidents*"

In addition, the DP Code was implemented in 2005 with an Enclosure (*Allegato*) A.5 entitled "*Deontological and good conduct code for the information systems managed by private subjects on the consumers' credit, customers' reliability and punctuality in payments*", specifically addressed to the financial stakeholders involved in the gathering and management of the citizens' personal data.

This deontological code is the result of private subjects' pressure (i.e. consumer associations and class associations), aimed to protect, through the DPA intervention, data relating consumer credit, as well as commercial activities in general. This code is addressed exclusively to private institutions (i.e. Banks, Credit Bureaus, Insurance Companies, Financial Institutes, etc.) and their related databases, excluding databases managed by public entities (i.e. Bank of Italy and Central Credit Register). This deontological code contains a set of rules aimed at defining the subjects entitled to gather, manage and store sensitive data on customers (art. 1-7); the consumers' rights to access their data (art. 8); management of Credit Scoring databases (art. 9); management of data from public sources (art. 10); security measures and devices to store sensitive data (art. 11); sanctions (art. 12); final dispositions (art. 13) and enforcement procedure (art. 14). In spite of this seemingly comprehensive coverage, private citizens are not aware of their rights and their abilities to exercise them. It is an entirely self referential, intransparent system.

As far as the *Redditometro* system is concerned, the DPA implemented an *ad hoc* provision, regulating access to the "Tax Register Information System" by banks and financial institutions. The Tax Register Information System is composed of sensitive data gathered from financial entities, aimed at collecting financial information for measuring the patrimony (incomes/expenses) declared by individuals, to verify the compliance of that information with their tax declaration (i.e. *Redditometro*). The final aim of this system is to reduce and control tax evasion. These rules have been implemented with a further DPA provision.

Finally, in response to public outcry about the system, the DPA has recently promulgated a provision, specifically referring to *Redditometro*. The original idea of *Redditometro* has been modified for compliance with citizens' fundamental rights, according to the Italian Constitution and the European Human Rights Charter (i.e. privacy and data protection rights). In particular, the DPA has defined certain rules for the application of the *Redditometro* by the Revenue Agency, to protect citizens' privacy:

-the inspection is addressed only on actual expenses, as it could not refer to estimated expenses. "Concrete expenses" are proved through evidence of payment (i.e. bank transaction, bank cheque, credit card transaction, etc.). It is possible to pay by cash, but in this case the amount is limited to one thousand Euros. This is called the "profiling principle".

-the Revenue Agency has to verify the composition of an individual's family, for the inspection of real expenses;

-the Revenue Agency should pay careful attention to the quality and accuracy of the gathered data, as the inspection needs to avoid discrepancies between the "fiscal profile of an individual" and the "civil status" of this person;

-the Taxpayer has the right to be properly informed that his/her personal data are subject to investigation, according to the *Redditometro* system (for instance, a specific clause in the tax declaration application has to be introduced to inform taxpayers on their personal data use and gathering);

-the *Redditomerto* system has to guarantee the "cross-examination principle", as the citizen has the right to prove the legitimacy of his/her expenses, in relation to his/her income (i.e. personal lifestyle). Besides, any taxpayer has the right to be informed about the consequences (e.g. sanctions) of refusing to provide the Revenue Agency with the documents to prove his/her legitimate expenses.

In *Norway*, Credit Scoring is entirely governed by Data Protection law and there is a system of licences granted by the Data Protection Authority to practice credit scoring. Nowadays, credit scoring is legally governed by Chapter 4 of the Personal Data Regulations of December 2000 (PDR), and in particular Sections 4-1 to 4-7. These outline the terms of credit scoring licences which are granted by the regulator.

Section 4-2 PDR provides a positive definition of the term "credit information service" as "activities which consist in providing information that throws light on creditworthiness or financial solvency" (1st para Section 4-2 PDR). The same section offers also a sort of negative definition by both identifying specific exceptions, and by making explicit all the services that "are not regarded" as such (2nd part 1st para, and 2nd para Section 4-2 PDR).

Section 4-3 PDR establishes rules for the "disclosure of credit information". The most important one concerns the limit to disclosure, stating that "[c]redit information may only be given to persons that have an objective need for it" (1st para Section 4-3 PDR). As we have already indicated, this wording is one of the most important shortcomings of the entire chapter, for at least two reasons. First, it is too vague, as it is not explicit what "an objective need" can be, and how this can be validated. "Objective need" is difficult to define without other elements, and the PDR does not provide more information, apart from in the Section 4-5, where it refers to Sections 34 and 35 of the PDA. Section 34 PDA obliges to "clarif[y] whether the processing of personal data may cause disadvantages for an individual which are not remedied by the provisions of Chapters II-IV [of the PDA, which define a series of rights of the data subjects and duties of the data controllers] and conditions pursuant to section 35". Section 35 PDA permits to "lay down conditions [in the licence] for processing when such conditions are necessary to limit the disadvantages the processing would otherwise entail for the data subject". Therefore, it is up to the Datatilsynet to carry on a sort of preliminary proportionality test on the types of processing foreseen by companies, and the same DPA has the power to insert specific conditions and limitations in the licence itself. The second reason is that the PDR does not oblige, explicitly, the enterprises providing credit

information services to check the request they receive before for disclosing the information. Nothing in the legislation prevents companies, once the licence is granted, to not respond to queries on credit information that could be considered non-legitimate. They have no explicit duty to check if the requiring party has "an objective need" for the credit information. Therefore, there is no specific filter to ensure that data are not unduly disclosed, but only an *ex post* control based on the data access provision discussed below. This appears to be one of the most salient features of credit scoring as surveillance in Norway, the very wide access based on the vague definition of "objective need".

Section 4-3 PDR also establishes as a general rule that information about credit scoring should be "provided in writing" to the person whose information is being processed. This procedure can be considered a safeguard for the data subjects requiring access to credit, as it creates a substantial trace of the effective use and result of credit scoring. As such, data subjects receive a letter informing them if someone (i.e. another private individual) has performed a credit check on them. Section 4-4 of the same act requires companies who perform credit scoring to do the same. The letter contains the kind of information provided about the person that has been assessed, the source of the information, who asked for the information (including address and phone number), and, if relevant, the name of the department or branch of the organizations asking for the information. Finally, the same provision further widens the data access rights of the data subject, as she can require "to be informed of what credit information has been provided about [her] in the last six months, to whom it was given and where it was obtained" (3rd para Section 4-4).

In theory, this Section is a key element of the entire Norwegian system. It provides a rather high level of transparency and ensures the awareness of the practices even when credit scoring is illegitimately operated. For example, secret credit scoring is practically inexistent, at least when this processing translates into the disclosure of information. Furthermore, this provision potentially exposes illegitimate requests of disclosure, but only when they are fulfilled. However, Section 4-4 PDR is far from being the perfect solution in terms of

awareness and transparency. As mentioned above, the copy of the disclosed data is only provided at the same time of disclosure itself, which practically means that there is no effective possibility for the data subject to oppose the release of her information in case of non-legitimate credit scoring. The only possibility is to complain *ex-post*, after the disclosure. Moreover, the awareness is not 'collective', in the sense that while each individual can become aware of the processing and disclosure of her own information, no clear picture of the size and main feature of credit scoring can be created. Indeed, the provision does not foresee the statistical aggregation of data on disclosure (e.g. how many, for which purposes…) or the publication of reports on the legitimacy of disclosures.

The second key element of credit scoring regulation is the ad hoc license system, administrated by the DPA. As mentioned above, the license system was already introduced at the time of the first Norwegian Data Protection legislation (cf. section 2.1 above). Following specific cases from *Personvernnemnda* and the DPA, the content of the licence was revised in a process started in 2009, and the final revised licence was finished in the beginning of 2012. The remainder of Chapter 4, Sections 4-5 to 4-7 of the PDR concerns this licence system. All enterprises who intend to conduct credit scoring have to seek not only a general permission, but a licence, which clarifies and limits, *inter alia*, the sources of data to be used, the different processing operations for different categories, the rules on the storage of information and data in specific registers. This licence-based system further strengths the powers of the Datatilsynet, which is the only authority that can grant the licences (1st para Section 4-5), and that can also "exempt the data controller from obligation[s]" derived from the same Chapter 4 (Section 4-7). Also, it is possible to state that each specific licence (based on a common template) becomes a sort of *ad hoc* data protection legal instrument.

The general licence application for the processing of personal data contains several requirements to be fulfilled. Once the licence for processing of personal data relating to credit scoring activities is given, the company receives a letter from the DPA stating more

clearly the rules for the practise and what the register can contain. According to Section §35 PDA, several requirements must be met. The register can only contain certain kinds of information, and this information is divided between information concerning data subjects and legal subjects, and also between credit information obtained from public and not-public sources. Some kinds of information are merely basic data concerning name (of data subject or legal subject), contact information and organisational number, whilst other types of information remain more vaguely defined: “commercial interest” (for data subjects) or “actual events of a natural and economic character that obviously matters” (for legal subjects). The DPA also states requirements concerning the sources from which personal data can be obtained. They generally include phone companies, media, other credit scoring agencies, Statistisk Sentralbyrå (SSB) and other public registers. Notably, the public tax lists, *Brønnøysundregistrene* and Norsk Lysningsblad, are among the public registers whose data may be collected. Further requirements concern also the process of actual disclosure, including the obligation of not marking ex post notifications with the company logo, and of using the fastest form of postage possible. The license also includes specifications about “objective need”, the possibility for “credit freeze” and the adequate routines for erasure.

When a case (either from a legal or natural person), leading to a decision at the DPA, is subject to complaint, the Privacy Appeals Board decides appeals against decisions. The *Personvernnemnda* is a Norwegian *sui generis* institution, which acts as an “independent administrative body subordinate to the King and the Ministry” that “shall decide appeals against the decisions” of the Datatilsynet (Section 43 PDA). While its decisions cannot be considered judicial case law, they have an important impact of the interpretation of data protection law, and, in specific cases, on the possible shaping of surveillance practices. Few cases directly concern credit scoring practices.

Within the *UK* the main piece of regulation guiding credit scoring is the Consumer Credit Act (1974). The Act requires those businesses dealing with credit to be licenced by the Office of Fair Trading (OFT). Credit companies in the UK cannot operate without the license and there

are approximately 120,000 license holders in the UK. If the OFT deems a business to be 'deceitful or oppressive or otherwise unfair or improper' then trading licenses are suspended or revoked. One of the main duties of the OFT is the prevention of 'irresponsible' lending (an emphasis added in the 2006 updated Act). Another legal provision effecting credit scoring has been the Data Protection Act (1988) also has a large influence on credit scoring companies as the information and privacy of individuals must be upheld and data must be stored and used in compliance with the act. Failure to comply has financial penalties.

With the expansion of credit-based financial products and advertising in social media, the Business, Innovation and Skills Committee state that there is a need for tighter regulation and compliance with the Consumer Credit Act in the financial services industry. One suggestion includes a call for centralized loan database, this is a 'real-time regulatory database' which is used by some US states (and some might argue in common with the centralised debtors list operated in Hungary). Lenders must log all loans and the repayment of those loans within the database and the regulations of the loans and credit histories of applicants can easily be verified. Undoubtedly ethical and surveillance issues abound with this model, but like most surveillance regimes it allows for ease of compliance and management. A phenomenon if current trends continue will remain prevalent for many UK citizens in the future.

Although each set of credit scoring practices are comprehensively goverened, in only Norway, and, to a lesser extent, the UK, are their clear pathways for citizens to exercise their rights in relation to credit scoring. The systems in Austria, Hungary and Italy are less transparent for citizens.

III.4.2 Participation

As is the case with ANPR, we see little evidence that wider stakeholders are meaningfully involved in the shaping of Credit Scoring practice. By contrast, however this is because as a practice it is already subject to heavy regulation with tightly defined stakeholders.

In *Austria* for example, the practice of credit scoring and rating by banks and credit agencies is accountable to regulatory organisations like the Data Protection Commission (DSK), the Financial Market Authority (FMA) or the Austrian National Bank. However the credit agencies are reported not to obey certain regulations. For example, they repeatedly and unlawfully refuse to delete data from their "black" lists. Several Supreme Court decisions have clearly established that subjects are entitled to have their records deleted from that list (cf. OGH 6 Ob 195/08g, 1.10.2008; OGH 6Ob41/10p, 15.4.2010). It is hard to find anything out about how the system operates from the outside.

In *Italy* the implementation of the credit scoring 'system' is tightly determined by close inter-organizational relations between Credit Bureaux and Banks/Financial Institutions. In practice. the content of the data-bases is based on an exchange of information between the Banks, which update their customer data monthly and transmit this to the Credit Bureau (i.e. CRIF) databases. Those managed by the other Credit Bureaus are available to the Banks for cross checking so that an *a priori* risk assessment can be made, before granting a loan to a consumer. The Consumer Associations have a marginal role to play and consumers in general are distrusted by financial institutions in Italy. They do not have a significant influence, although they are often used as an additional publicity/information channel to improve the customers knowledge when they are subject to the credit scoring system. For example the consumer association *Altroconsumo*, in collaboration with CRIF, drafted a handbook for consumers about the practice. Similarly the *Federconsumatori* in Sicily and the Presidency of the Sicily Region, 2009, drafted another handbook addressed to the Sicilian citizens to inform them how to access the credit market. Close-knit organizational ties and low transparency of the central debtors list is also the case in *Hungary.* Banks have unilaterally reformed the credit scoring system in Hungary without reference to external laws or regulations.

By contrast, the case study of *Norway* highlights how data protection and credit scoring co-constitute, rather than work against, each other. The two are entangled to the point that it is impossible to analyze the one without taking into account the other. As such, all challenges come, legitimately, through the data protection channel, which is highly transparent to, and at the disposal of, the public and to other stakeholders. For example, as well as private companies performing credit checks, private citizens have done so as well either as landlords or in other court proceedings, such as divorce.

When a case (either from a legal or natural person), leading to a decision at the DPA, is subject to complaint, the Privacy Appeals Board decides appeals against decisions. The *Personvernnemnda* is a Norwegian *sui generis* institution, which acts as an "independent administrative body subordinate to the King and the Ministry" that "shall decide appeals against the decisions" of the Datatilsynet (Section 43 PDA). While its decisions cannot be considered judicial case law, they have an important impact of the interpretation of data protection law, and, in specific cases, on the possible shaping of surveillance practices. Few cases directly concern credit scoring practices. For example, a joint complaint in 2012 by several credit scoring agencies' requested to add new sources of data to their existing pool. In this case, Personvernnemnda partly took the appeal into account, by including two out of four disputed sources of information in the license. In 2009, a request by journalists concerned the possibility to access credit scoring information as part of research for a television programme about consumer rights. The complaint was not sustained. Another case from 2009 regarded the scope of the powers of the Norwegian DPA vis-à-vis credit scoring agencies' access and processing of specific data sources. The judgment was triggered by a complaint by a company sorted in the highest category of risk based on the fact that they recently changed their daily manager of the company. Following, the complaint had to do with the weighing of the information from different sources. The DPA concluded that neither the PDA, the PDR nor the general licence regulates the weighing of the various information that credit scoring companies can legally obtain. The DPA concluded that they

did not have the competence to assess the weighing of the different factors, and this remained the responsibility of the credit scoring agencies. The Personvernnemnda upheld the position of the DPA and the complaint was not sustained.

In the *UK* once again we see tight inter-organizational relations through which credit referencing data are shared. Many financial organisations also share, for example, credit card information - HBOS, Barclaycards and MBNA share 'full data', which includes debts, any missed repayments, the amounts normally repaid (if minimum or full payments are made monthly) and any promotional deals customers may enjoy. It is the culmination of all of these factors which ultimately secures financial loans. The British Bankers Association (BBA) acknowledge that there is a transfer of knowledge between banks and 'Credit reference agencies'. The agreement is of mutual consent; banks provide financial information on individuals to the agencies which helps in the calculation of credit scores and the agencies provide banks with scores based on the amalgamation of information from numerous sources. The agreement is optional, but the benefits are clear. To eradicate issues of data protection, information is only passed with the consent of the customer, banks stipulate to customers when opening an account or applying for credit that the customer's information may be shared in helping the bank to reach consensus on credit suitability. The banks however do limit the information disclosed and it is confined to:

1. Whether a customer has fallen behind with their payments; and
2. When the amount owed is not in dispute; and
3. When the customer has not made proposals satisfactory to the bank concerning means of repayment following a formal demand; and
4. The customer has been given at least 28 days' notice of the bank's intention to disclose information.

Some banks also share performance data about their customers to further support responsible lending. Exceptions include, for example, criminal activity when information is disclosed to the police with or without consent. Although the system is quite closed, consumers are well informed and if they ask a question of a bank concerning their credit score, the bank is obliged to answer it.

In summary, stakeholder participation in credit scoring is restricted to a tightly delineated set of relationships between financial institutions, financial regulators and credit bureaux/agencies. These relationships focus on protecting the commercial efficacy of the financial institution and, with the exception of Norway, limit challenge and external scrutiny of the practice.

III.4.3 Engagement

We now focus on the mechanisms through which consumers become aware of credit scoring so that they can intervene and manage the way in which they appear in the databases. Subject access requests, publicly available information and media coverage were the focus of the analysis. We argue that because credit scoring is almost an aspect of financial services infrastructure, its internal workings and implications are not routinely questioned. It only becomes an issue if a consumer is prevented from obtaining credit because of a problematic credit history. Consequently, from the citizen's perspective the outcome will be a reduced level of awareness. Furthermore those categories of subjects who are not able first to find, and then to understand, highly technical information about credit scoring, as well as specific financial market regulations are excluded altogether.

However, we begin with an amusing anecdote from the United States, which reveals exactly how high consumer awareness of credit scoring is in that country. In December 2012 the New York Times ran an article about how even Cupid has an interest in credit scores. As the Times explained for a couple on a date the awkward etiquette of when to ask 'how is your credit rating' inevitably arises. While the question may seem crass and preposterous to

several audiences, the practical implications of the question to some New Yorkers have consequences that they simply want to know about. If a person has poor credit, there are potential financial implications for the blossoming relationship; for example the negative effect a poor credit rating would have if the couple where to buy a home together. The New York example goes someway to highlighting the societal impact credit scoring is inducing in how we now live our lives. Financial capacity, it can be argued, has always played a role for Cupid (just think of how dowries work) and for some it may seem strange that it has taken this long for credit rating to come to the fore in the 'dating' world. However, what may be more startling is the growing prevalence and influence of this type of rating system. Awareness across Europe differs greatly, and we now will review some of the evidence.

In *Austria*, banks are governed by a historical principle of administrative secrecy, and this principle binds all employees. Therefore they are discouraged from sharing any aspect of their practice with customers or others outside the institution. Lip service is paid to transparency, therefore. Several large credit agencies and organisations like the KSV1870 or CRIF offer information on their websites, including details on subject access requests or name and function of different services, databases and warning lists. According to the Austrian Data Protection Act, consumers have the right to request a copy of all data held on them by the credit bureau. This is for free once a year and has to be done within 8 weeks. During the course of the study two subject access requests were conducted by one of the researchers; one at the KSV1870 and the other one at CRIF. Both were free of charge and delivered in the time period delimited by the data protection act. However the information shared was disappointingly sparse. The KSV1870 listed the researcher's current post address and a few service companies, which are involved in the processing of one's data. The CRIF revealed all the main addresses of the researcher since their birth. In both cases they revealed no further information on how they use these data or how, for example, the researcher's current postcode is used and weighted in the rating process. They also claim not to have saved any payment data on the researchers' transactions. CRIF Austria also

informed the researcher that about 10.000 subject access requests have to be answered each year. There is the possibility of compensation for illegal or wrong entries in 'warning lists' and databases. If an interested party is harmed by an entry in such a database, because they cannot claim, for example, a cheap mobile phone offer and therefore needs to choose a much more expensive option, he can hold somebody accountable for these damages (Credit damage according to § 1330 ABGB).[92]

When individual banks were approached for information about to their credit scoring processes, however, nothing whatsoever was revealed. The researchers found it extremely difficult to uncover any kind of information, directly from the banks, which related to the practice. Effectively, its existence was denied and it was treated as a trade secret. While the customer is entirely transparent, the rating system itself is not.

Discussions around credit scoring in the Austrian media refer to how it sometimes prevents private citizens and SMEs from getting credit. Occasionally there are reports on data protection problems. A case of unauthorized data reselling in judicial circles was recently taken to court. The most recent mass media coverage which implicated credit scoring referred to how lending guidelines were becoming more strict in both personal and corporate markets, and how particular segments of the population are more likely to be indebted than others. Two newspaper articles in the last six years have focused on creditworthiness, credit blacklists and the information which informs consumer credit scoring.

In *Hungary* individual engagement with credit scoring via the legal system did not occur very regularly either. The researchers identified only 48 cases having some connections with processing of personal data for credit-scoring purposes. Only 32 of these lawsuits could be considered as relevant from our point of view since the rest of the cases did not reveal any

[92] http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=30575bvj (accessed 20 Nov. 2013).

objection on the plaintiff's side to this form of surveillance (e.g. legal debates among financial institutions, questions of legal interpretation) or had to be left out for other reasons (e.g. lawsuits filed by legal persons).

However, the media do report controversial issues which have arisen around credit scoring. Most of these relate to poor administration of financial products. For example, earlier discussions of the unlawful retention of identification documents by Citibank feature, and the mistaken opening of a bank account for someone who had been refused a loan were uncovered by the national news media. Other stories concern incorrect listing of citizens on the bad debtors list and the unjust termination of leasing contracts. Articles about the advantages of the positive debtors list reflect, understandably, the approach of the financial institutions; communiqués about its disadvantages and questionable legal grounds were issued mainly by the Parliamentary Commissioner for Data Protection and Freedom of Information, reflecting his position (until the abolishing of his office), while news and articles about complaints and court cases generally present the complainants' aspects. Longer analyses in the latter subject often include interviews with competent experts from the financial institutions, too.

In *Italy,* the individual consumer may engage to a greater extent with credit scoring because of the more informal way in which lending takes place when compared to other case study countries. The contact between the Bank and the customer/citizen is frequently established through a Private Banking Consultant, i.e. a direct, face to face relationship between these two subjects for the advantage of both the parties involved in the credit procedure. The Bank needs, to a certain extent, the personal contact with a (potential) customer, as it represents one of the privileged channels of surveying to collect qualitative and quantitative information about the client's life, profession, activity and patrimony, which can help the Financial Institutions to make an effective risk assessment in case of a loan request. On the other hand, the citizen has a direct channel of information from the Bank, to whom to address

his/her requests, as well as freely explain the necessities in his/her everyday life. Therefore, the “rating models” developed by the Banks for the credit market are implemented and updated on the basis of the information exchanged and collected from the direct interaction between the Bank and the client, rather than an automated system as is the case in the UK. In fact, whether the citizen needs to apply for a loan or find out why they have been denied a loan, the Private Banker Consultant can give the client an answer about his/her rights and financial “profile”. In particular, the client of the Bank can also request information about his/her personal “rating”, calculated by the Bank (through an algorithm model) and the Bank is obliged to answer this question, although it will never give a detailed explanation on the model at the base of the “rating system” developed by the Bank itself.

The Credit Bureaux and, in particular CRIF, have also implemented several channels through which they may be contacted directly by the citizens/customers, although CRIF has no direct relation with private individuals, having only contracts specifically stipulated between the Banks/Financial Institutions and CRIF itself. Therefore, contact with the citizen is necessary when there is an objective need in communicating modifications, updates or complaints on the personal data gathered by the CRIF database system.

The citizens can access their own data at three different levels during the whole Credit Scoring procedure, according to which stakeholders the request refers to, although the access through Consumer Associations is not statistically representative and almost non-existent:

1. personal data access requested directly from the Bank and/or Financial Institution
2. personal data access requested from Private Institutions, i.e. “Credit Bureaus” (CRIF and EXPERIAN)
3. personal data access requested from the Consumer Associations for accessing the “Credit Bureaux” (CRIF in particular) databases

Each stakeholder has its own procedure in accessing data depending on the natural subject that the data belongs to and the procedures are substantially based on the DPA dispositions, referred to in the legal and provisional sources, i.e. the DP Code and the Enclosure A.5 of the DP Code.

However, although there appear to be many channels, the access procedure is not very efficient. It is the case, for instance, for the data subject to gain data access through the Consumer Associations, although through this one can only access the Credit Bureaux (e.g. CRIF) databases access and the procedure is strictly regulated. Most consumers prefer to contact the CRIF or EXPERIAN personally, firstly to shorten the whole procedure and because of the lack of information about this service (i.e. CRIF website). It is also important to note that the rate of access requests through these kind of associations is extremely low, almost marginal for the statistical data gathered by CRIF. Finally, as in the case of Austria, the information revealed is piecemeal and does not contain any detailed information about financial transactions or the basis upon which the credit rating is calculated.

The most important national mass media in general, as well as the specialized newspapers (*Il Sole 24 Ore*, *Norme & Tributi*, *Plus24*, etc.) in Italy have a limited interest in the Credit Scoring issue, as their attention through the years (from the '90s, when the practice of Credit Scoring was introduced in the Italian financial system) has always been devoted to the "rating system" applied to Companies and Corporates (legal subjects), rather than private citizens/consumers (natural subjects).

The situation is somewhat different in relation to the tax compliance system, *Redditometro*. The diffused perception of this instrument has been the creation of a "Big Brother" effect, where the citizens are "spied upon" by the State, able to monitor the lifestyles of its citizens, who are forced by the necessity to justify any expense/income or investment in their private

life. The mass-media have paid great attention to this issue, describing it as an invasive tool into citizens' privacy, through the exploitation of the banks' databases and information gathered from their customers.

At first, mass-media focused their attention on the new set of rules implemented by the Revenue Agency: i.e. the procedure of inspections, the timing of inspections (from 2009 on), the cross inspection based on the lifestyle of the citizen (i.e. personal patrimony) and the data gathered in the "Tax Register Information System", etc.. The Revenue Agency has now direct access to both bank accounts and financial investments of customers

.

A second aspect pointed out by the mass-media is the legal framework. The implementation of the *Redditometro* provoked the reaction of citizens challenging the system from different perspectives: namely, the validity of the statement of assets and liabilities for tax investigation, which has been discussed by the Province/Regional Fiscal Commissions, right up to appeals to the Supreme Court (i.e. *Corte di Cassazione*); the potential infringement of personal data and citizens' privacy, through a direct access of the *Redditometro* instrument to several databases of private and public institutions, (*primus inter pares*, the bank and financial institutes' databases).

As expected, the case is somewhat different in *Norway.* While credit scoring can be considered a mundane experience for many individuals, awareness is formally built into the practice itself: both *ex ante* and *ex post* the credit check. Generally the person requiring a service has to consent to be credit checked before the service provider can send a request to one of the credit scoring companies. Then, after the credit check is carried out, the credit scoring company has to send a notification to the person at stake. This latter operation is mandated by law, and ensures that even illegitimate credit scoring is notified to the relevant data subjects (with the potential exception of abuses by credit scoring companies' employees). Compared to other surveillance practices involving forms of profiling, the *ex*

post notification system is a specific feature of credit scoring. Still, in cases of illegitimate requests of credit scoring, this sort of 'awareness by design' cannot prevent disclosure, and only permits to data subjects to complain after surveillance has taken place.

When it comes to data protection issues, contacting the DPA is generally considered the first step for data subjects considering lodging a complaint. From the annual reports by the DPA, we can read that in 2010 the DPA handled around 1600 cases, mostly from natural persons, asking if the PDA had been respected in different cases. Use of CCTV, disclosures of full birth number and credit scoring were the main themes. Regarding the latter, the issues at stake concerned mainly data subjects not being able to understand why credit scoring was necessary in specific cases, or not understanding why they had been subject to credit scoring at all. Thus, similarly as it was the case for the controversies in the media, most of the issues and complaints coming from data subjects focus on illegitimate disclosure, rather than radical opposition to credit scoring.

On the other hand, a potentially radical form of opposition to credit scoring is not only available but also institutionally publicized by key stakeholders: the so-called *kredittsperre* or 'credit block'. Individuals can formally prohibit credit scoring agencies to check them, and thus to never accept demands to do so from third parties. Even if they do not formally or institutionally question the surveillance practice in itself, they oppose to it in a pretty radical way: they opt out and limit its reach. As access to credit-related services is not possible anymore, a credit block emphasizes and exposes the pervasiveness of credit scoring and its embedment and impact on everyday life.

According to the media, the reasons for setting up a credit block can be manifold. For example, it prevents ID theft, since a common way to commit identity theft is to raise a credit in the victim's name. Another reason can be to put limitations to personal consumption, limiting their ability to order credit cards and contract credits. To avoid unnecessary credit and "snooping" is another reason. Employees of companies that have access to credit information (employees of banks, financial institutions, and companies with agreements with

credit information agencies) can use the access to things other than just checking customers. The DPA reports of having received a number of cases where people have been credit checked during courtship, child custody and divorce.

In the *UK* a considerable amount of information is available to the public as to how they can manage their own credit score. A plethora of websites offer advice on financial matters, as well as, newspaper supplements, television and radio programmes. Within these formats there is often a clear focus on how to improve one's credit score. The emphasis is effectively on how to play the system to your advantage. It is possible to pay a small sum of £2 to get a copy of one's credit record and see what needs to be changed. Advice suggests that if one wants to borrow money there is no escaping the credit score, everyone has one and that the first thing a lending organisation will do is check your score. Therefore it is essential that customers come to terms with what their credit score is and how to use it. Commonly cited tips for managing one's score, from the British media, are found in box III.1:

1. Make sure you are on the electoral roll and create a good credit history
2. Be attentive to debit
3. Look at your file and correct mistakes
4. Credit reference agencies don't know about the following, therefore there is no need to worry about them:
   Parking or driving fines; Council tax arrears; Race, religion, colour; Whether you've checked your file; 'Soft searches'; Salary; Savings accounts; Medical history; Criminal record; Child Support Agency files; Information on relatives; Student loans; Declined applications; Some defaults or missed payments - these stay on file for six years.
5. Avoid the rejection spiral
6. Be consistent on applications
7. Don't put too many applications in at once
8. A customer is scored as an individual
9. Use a 'quotation search' not a 'credit search'
10. Don't lie on the application

Box III.1: How to manage a credit score

Because of the public awareness campaigns around credit scoring in the UK, the researchers conducted an in –depth interview with a financial services consumer and his experience with credit scoring and 'playing the system'. The instance he speaks of revolves around buying a piece of furniture about 10 years ago when credit was refused. The

interviewee knew he had enough money in the bank meet the minimum guarantee levels and so was confused by the refusal. Therefore he began to run through the possibilities of why it may have been refused.

> *That was one of those triggers and I just said, no. I need to actually just… I need to really figure out how the hell this functions. What exactly are the criteria which are being used? Also, I had a vague understanding that I had to look at where exactly they were collecting the information. What are the sources? What are the points where the information is being fed through it? This is where it became a factor. Also, how you can… what can I do in order to create a credit history…*

The trigger mentioned spurred the interviewee to question how the system works and to gain a better understanding of its workings. He had suspected his name (which to a UK audience is unusual) was problematic, particularly as it was commonly misspelled and there various accounts, for instance, for gas or electricity did not match his bank account. Also the dispute with a phone company he also suspected was to have a knock-on effect on his credit score. All of which encouraged him to seek out further information. He elaborates on his awareness at the time

> *I think I would say that I was aware of it. I was a little bit apprehensive about using it and hence – because of that – it was to my disadvantage personally because of our complex last name and name. There are frequently problems in how it gets actually reported. So, what happens is… for instance, one of the elements which is used for credit scoring here is being registered on the voter's register and I was. One of the credit scoring agencies was not using that. So, what happened is… I couldn't figure out why it is that my credit scoring wasn't giving me the kind of… for some reason I got turned down on one or two occasions for credit despite the fact that when I was offered a credit card, what I was asking was well within the realm of my ability to pay.*

Highlighted in the comments are common problems faced when securing credit; errors in the system or contracts being cancelled. These as we have seen have consequences and present tensions and ruptures in how the system worked for the interviewee. The interviewee believed there was an element of control in how a customer can maintain and improve their financial capabilities and credit scoring is one example of how this can be achieved.

> *For me it's the tool that allows me in my life to increase my ability to raise finances, expand my ability to use various lines of credit… generally speaking it gives me a hell of a lot more flexibility. By the way, I just had my credit increased today. So, it's a subject close to my heart and increasingly has become a tool in itself to use as an advantage to me. So, I became almost anally compulsive about what exactly I can use in our favour just so we can have more flexibility and this process has started about seven or eight years ago roughly when I started working at the university where I started getting into the fine detail.*

Nevertheless, the interviewee's thoughts are also balanced with scepticism of how his information is being processed and analysed. As he states,

> *It is definitely a form of surveillance. It's definitely a form of monitoring. I have no means to avoid it, so I needed to find a means to control it or not necessarily control it so much as to massively influence it in passive and active ways….. We don't want to really have a car. We're living in a place where we don't need one, but… I want to have the freedom to buy a … car. I want to have the freedom to say, I don't have one because it's a choice or I want to be able to go to Australia for a vacation, but I want to make that choice.*

As the interviewee recognises there is a dilemma between proportionality and necessity. One must recognise you will be credit scored when availing of certain products, however

there are issues concerning privacy and the intricate details that may feature in how credit scores are complied.

> *I don't know whether it's proportional. If it's applied carefully and honestly on both parties – because it's a contractual reality – then it can be that. However, if it's applied as an abuse of authority – and it can be like that, too – it can be absolutely detrimental to people's reality … On one hand this is like a financial miracle alter-ego, but in practice it really opens up phenomenally the opportunities that you have. So, what I was really paranoid about is that at any point there is no financial downward spiral because the same thing that occurs with positive stuff where it gives an inflated positivity… it also happens in the other direction and to me that spells reduction of freedom, reduction of choice, reduction of status almost, and not status in the sense of… I get a really blingy kind of thing, but to me it's more about status in the account of opportunities that you're going to have for yourself or your family.*

What the interviewee highlights here is an instance that made him question how he gained credit and how he was evaluated when applying for a financial product. The initial refusal led to him gaining a greater and more in-depth knowledge as to how credit scoring works. This in turn has allowed him to use it to his benefit. However, while gaining 'back' control may have been a motive and as he recognises it is a form of surveillance, the problematic and resilience here is centred on using the system to your advantage and not questioning how they system works.

Our examination of public engagement with Credit Scoring reveals that in Austria, Hungary and Italy there is a huge gap in the public understanding of credit scoring. While Norway and the UK are keen to educate the public on the importance of credit scoring, this is for very different reasons. In Norway it is possible to opt out altogether, to challenge credit scoring and to use it for personal ends. In the UK, the tenor of public engagement is to educate citizens in banking practices so that they to become better financial citizens, rather than to

encourage them to challenge or opt out of the practice. These patterns are reflected in the attention given to credit scoring in the mass media. There is a lack of interest in the issue in Austria, Hungary and Italy. In Norway, mass media devote attention to specific aspects of CS, such as the prevention to ID thefts, and avoiding unnecessary debts. In the UK the mass media give a considerable attention to CS, since they underline the social impact of this practice and its influence in consumer choice, as well as how consumers can play the system to their advantage.

III.5 Improving democratic resilience in the face of Credit Scoring

Although there are substantial difference between the countries in terms of financial traditions and procedures, we note some similarities in terms of democratic intersections with credit scoring. Austria, Hungary and Italy are similar in that there are strong cultures of secrecy (Austria), resistance to external regulation (Hungary) and in some contexts, active disrespect of regulatory efforts in relation to credit scoring practice (Italy). These are also countries in which consumer access to credit is not seen as an essential part of life, unlike in Norway and the UK. Because credit scoring is effectively the oil which lubricates the consumer finance machine, it operates in an invisible way for most consumers. They only become aware of credit scoring if they have a negative rating and are prevented from obtaining credit: when the oil runs out – to continue the metaphor. In Norway and the UK, the system is more open to citizen's involvement. However in Norway this involvement starts, from first principles, with data protection, whereas in the UK the emphasis is on making credit widely available whilst simultaneously educating the public about its dangers. Data protection does not widely feature in the British regulatory context.

In the majority of cases, it is therefore difficult to assess whether credit scoring as a surveillance practice is counteracted by democratic practices of governance, participation and engagement. This is because the surveillant aspects of credit scoring are not an issue except for in Norway where it is fully recognised from the outset. The distributive justice

aspects are an issue, however. It is tempting to argue that distributive justice concerns arise if consumers are denied credit, but in Norway it was fully understood that one's postal code, age, or other factors may reduce one's credit score even if one has never missed a payment. Distributive justice is an issue which is endemic to credit scoring and in Austria, the consumer protection agency and various NGOs strive to make consumers aware of credit scoring but are really at the margins of public debate. Decisions about the shape and future of credit scoring are taken in the elite contexts of high finance and government. In Hungary there is no direct involvement of any parliamentary or citizen representatives in credit scoring practices as banks, whilst mandated by statute to operate the central debtor lists, do so on a self-organized basis. In Italy there is hardly any perception of credit scoring as surveillance (if at all) and with a weak consumer association there is little room for campaigning or awareness-raising about the practice. Where financial information is shared for tax purposes, however, the situation is completely different. In Norway, there is no discussion of surveillance practice either, but that is because any questions about the surveillant intentions behind credit scoring are counteracted by the process being completely open. The Norwegian case is an example of how democratic processes, set within a rights framework from the outset, can counteract some of the more secretive and intransparent ways in which credit scoring is practiced in other contexts. It is always clear to citizens when they are being scored and by whom. It is possible for citizens to withdraw their consent at any time. Problems arise, however, where the system is abused. There is little in place to prevent that happening, with remedies only being available afterwards. However the notification system ensures that such abuses are detected immediately. Finally, in the UK, a high level of citizen awareness enables individuals to use credit scoring to their advantage and to manage their own score actively. However there are other abuses of credit scoring by irresponsible lenders in the UK which merit particular attention by regulators. With the exception of the Norwegian case and to a lesser extent the British case, credit scoring becomes controversial because it is a powerful means by which economic opportunities are distributed. At the same time it enhances the power of financial institutions to determine

those opportunities whilst marginalising the power of regulators and other consumer interest groups.

In terms of opportunities for democratic resilience, it seems that, in Austria, Italy and Hungary financial institutions are rather resilient to democratic practices of governance and participation. In turn, these practices would normally demand that institutions are more open and accountable to the citizens and government for their credit scoring practices. Commercial interest and secrecy seems to trump these ideas, however. We observed a centralisation of power in financial institutions which, from a democratic point of view, is problematic. Institutional level intervention either through governance or participation would break these practices open. However this is not a particularly realistic suggestion, not least because governments of all persuasions need to be careful how they approach the powerful financial services sector. Ironically a serious harm, controversy, or shock is required to wake up regulators to the power of credit scoring because of its basis in social sorting. An alternative strategy would be for an engaged mass media to make more of the distributive justice consequences of credit scoring, as it has in the UK and in Norway. In these two countries, the emphasis has been different. In the UK, credit scoring is part of controversial 'irresponsible lending' practices which are currently receiving huge amounts of media attention. In Norway all manner of misuses of credit scoring are reported, and, ultimately, debated to ensure that the practice is even better regulated. We see everyday public engagement with the consequences of credit scoring as the key, particularly if consumer credit is set to expand.

CHAPTER FOUR

NEIGHBOURHOOD WATCH

IV.1 Neighbourhood Watch: An introduction to the practice

Neighbourhood Watch is conceptualised in this project as a 'horizontal surveillance practice' where citizens watch each other. The original concept of Neighbourhood Watch is claimed to have grown as a community-based response to the murder of Kitty Genovese in New York in 1964 in which a young woman was raped and murdered.[93] Despite her cries for help (for around 30 minutes) having been heard by more than 30 neighbours, nobody apparently summoned help for her or went to her aid. The inaction of the bystanders in this murder led to studies of the notion of 'bystander intervention' or 'bystander non-intervention' a feature of which is that people acting as part of a group are less likely to intervene in such a situation as would an individual acting on their own. However, the origins of neighbourhood watch in the United States of America are probably not just due to the inactivity of the bystanders in the Kitty Genovese murder, but are more likely to be attributable to a number of other factors. These factors range from the generation of a range of societal responses in seeking to protect homes, apartments, passengers on underground transport systems etc., or as a response, as Titus suggests, to the 'burglary epidemic' in the United States.[94]

In the Anglo American tradition, Neighbourhood Watch thus comprises informally organized local neighbourhood groups looking out for all kinds of wrongdoing, in the spirit of community safety and to assist the police. However, these kinds of social practice take on a completely different kind of significance in European countries which have had fascist or authoritarian

[93] Platt, John, Social traps, American Psychological Association, 28, 8, 1973, p.641.
[94] Titus, Richard M. (1984) Residential burglary and the community response, Springer, 97, pp.97-130.

pasts. In this case study we explore the operation of 'neighbourhood watch-style' schemes in Austria, Germany, Spain and the United Kingdom.

IV.1.1 The history of Neighbourhood Watch (NW)

In this section we examine the concept of Neighbourhood Watch in each of the case study countries. It is quite clear that, apart from in the UK, these schemes are controversial because of their historical significance. The picture is complex and fragmented everywhere except the UK.

In *Austria* Neighbourhood Watch schemes in the Anglo-American tradition are rare. Austrian culture and history has shaped how local crime problems are perceived and responded to. Austrian culture still contains elements of the authoritarian monarchic spirit rooted in the old Austro-Hungarian Empire and Austrian police only recently changed their policing style from military to professional. The concept of community policing is hence in its infancy and given the cultural heritage, it has only had limited success.

In Austrian political culture security has always been perceived as the task of the State and so the active involvement of citizens in local security matters has not developed. Citizens were expected to report matters of suspicion to the police rather than actively get involved themselves. There is one prominent character in Austrian popular culture who embodies this type of mentality: the concierge (*Hausmeister*), who was controlling the tenants in city dwellings, registering every new tenant and even visitors and acting as a low-key surveillance operative for the police.

However there are some NW-like organizations in Austria who attempt to undertake citizen-based surveillance and control. Three different types of organization were identified: bottom-up, municipal, and administrative. The main characteristics of each of these types are briefly described below.

The *Bottom-up approach* is characterised by 'Pro-Neighbour'. Pro-Neighbour is a grass-root movement, initiated by a retired Viennese citizen after more and more burglaries were committed in his neighbourhood. He started the campaign in 2007, approaching neighbours, local police and city council members. Rallying for his cause he managed to establish a core group of activists and received attention from local media. Today he runs a stable network of activists exchanging information and collecting "intelligence" in a loose cooperation with local police forces. Fostering communication processes amongst the members of Pro-neighbour and the (loose) cooperation with local police forces are the backbone of the initiative.

Municipal security forces called 'City Watch' were established as part of a political campaign, by various conservative parties, at the communal level. They were supposed to act as a kind civil order force, mostly focussing on incivilities and disorder problems. From a legal perspective they have no police power and primarily they are supposed to increase perceived security in public space.

Administrative approaches emerged in Vienna's social housing stock, which is extensive. Since the 1920s Vienna has maintained its public housing with about one third of the population living in apartment buildings (approx.. 200.000 apartments in 2000 housing complexes) owned and managed by the City of Vienna. "Wohnpartners" are a mobile concierge service-cum-social worker catering for the mostly multi-cultural resident population of Vienna's public housing. One could see these figures as second-order vigilantes, trying to convince residents to watch over themselves in a non-aggressive manner, but watching their neighbours nonetheless. One of the main reasons for the introduction of Wohnpartners in 2010 was the increased cultural mix in the public housing estates with migrants flowing in after the fall of the Iron Curtain in 1989. The self-declared objective of this scheme is to focus on three main tasks: conflict management, community outreach, and networking.

In a manner similar to Austria, in *Germany* the establishment of internal security *("innere Sicherheit")* in general or community safety in particular has always been the domain of the

police. As a result, Neighbourhood Watch schemes, or more broadly, any activities or initiatives concerning public safety that were based on civil engagement, rarely exist. If they do exist, they are very heterogenous regarding their purposes and methods. At times, however police have guided the active involvement of citizens in the field of crime prevention and the surveillance of suspects. Understanding these phenomena is tricky: Patterns are difficult to establish because policing operates differently in each *Land* and so each police force approaches this issue differently. Furthermore, whenever citizen involvement in community safety is proposed a standard set of arguments is deployed to dismiss the ideas. References to "right winged vigilantes" and left wing "civil patrol" or "militia" are commonplace. We first examine the institutionally-influenced approaches and then move on to those based on civil engagement.

Historically, there were three phases of institution-based neighbourhood watch which have contributed to its controversial position in Germany today. First, the *"Bürgerwehr"* which are local or regional defence associations against external threats, as well as police-like forces that control internal security. They have their roots partly in the Middle Ages and today exist only as cultural, folkloristic clubs focused on preserving tradition. Nevertheless the term "Bürgerwehr" is still a sceptical way to describe initiatives that resemble neighbourhood watch schemes. Over the years political parties, police forces and the military have attempted to co-opt the *Bürgerwehr* for surveillance and security purposes, which is why they are treated with scepticism as a community safety group. Second, during the national socialist regime The *Blockwart* was the most notorious neighbourhood watch institution. The Blockwart placed personnel in all kinds of apartment buildings in towns and cities and they would spy on all of the residents there. Historical research discusses at least critically the thesis, that "the Blockwart's contribution to the stability of the NS Regime was even higher than that of the Gestapo".[95] A character similar to that of the Blockwart figure was also existent in the Stasi-Regime of the GDR: It was required to register every (short- and long-

[95] Weyrather, Irmgarth: Die braune Fassade, Über d. Zusammenleben von Nazis, Kommunisten, Juden, Sozialdemokraten, Bürgern u. Arb. im Berliner Mietshaus, Literatur und Erfahrung 3 (1982, 10). S. 44.

term) visit of non-house residents at the "Hausvertrauensmann" (i.e.: "Trusted House Resident"); especially visitors from outside the GDR had to provide evidence for where they have spent their nights during their stay. Third, *The Post-War 'Volunteer Police Service'* was a feature of Germany's rebuilt security institutions. The Blockwarte no longer existed and the Bürgerwehr were relieved of their surveillance or security functions. Some Länder introduced volunteer police, who underwent some police training and had uniforms but had restricted duties. Community crime prevention was only added in 1998 to its duties in Baden Würtemmberg. In Bavaria, Saxonia and Hessen the "volunteer police service" was introduced with community crime prevention as its main mission. This police service is entitled "Sicherheitswacht" (security guards). After unification, the Berlin Sicherheitswacht had to be closed down because right wing extremists were very active in the service. More generally Sicherhietswacht has been criticised as a cynical money saving exercise, as a harbour for right wing extremism and because it is ineffective at preventing crime.

There are some neighbourhood watch-style organizations operating in Germany today which are not directly connected to the police.

Kiezläufer (Hamburg, Berlin) are people that walk around certain inner city areas. The term "Kiez" corresponds to "neighbourhood": A spatially limited area, producing a sense of belonging. In some cases a Kiez has some infamous elements: a good example is St. Pauli in Hamburg. It's a term most commonly used in Northern Germany. The idea of Kiezläufer is born out of an institutional arrangement called "Stärken vor Ort" ("Strengthening on site") funded by the *Bundesministerium für Familie, Senioren, Frauen und Jugend (ministry of families, pensioners, women and youth)*, the European Social Funds and the European Union. The idea did not come from the Kiez-locals, but was introduced by Hamburg Police, the Institut für konstruktive Konfliktaustragung und Mediation (IKM) and an organization called "Get the Kick e.V." Locals, particularly those who had worked with young people, became Kiez agents. In Berlin, their remit is to counter vandalism, violence, fly-tipping on

streets and in parks. Generally, all Kiezläufer organisations have an institutional structure and the Kiezläufer themselves must be trained, registered and report their work to the police. The project “Wachsame Nachbarn” (alert neighbour), has also been initiated by the police as a reaction to the increasing numbers of burglary all over Germany in 2004. Since then the initiative regularly appears in the newspapers, especially when statistics about burglary are rising. It’s one of a small number of such projects which can be found in the whole country. Wachsame Nachbarn aims to inform people about security measures against burglary. They encourage citizens to watch over their neighbour’s house and to speak to people passing through their neighbourhood that obviously do not come from that area. The project is focused on establishing security within an urban quarter. It is not focused on community life, but seeks to protect the houses of the residents from external threats. Stickers on postboxes and houses act as a deterrent to burglars. Citizens share their observations on the project’s website and residents can become informed about current issues in their neighbourhood. To share observations, citizens have to register to the site and prove that they are a resident.

Nachtwanderer (“night wanderer”) is probably the initiative that is least influenced by the police or other institutions. Based only in Northern Germany, and ussing an idea developed in Sweden in the late 1980s, its focus is on observing young people in public places, clubs or on public transport, to prevent conflicts. Parents or other residents tend to be *Nachtwanderers*. The three main goals are to really get in contact with the young people (not just passively observing), but respecting their privacy; to not solve serious trouble on their own, but call the police instead; to discuss all incidents within the organisations and protocol these discussions. Members of the “Nachtwanderers” wear uniforms and logos. There is no regular exchange of information between the single Nachtwanderer organisations, so it really stays at the neighbourhood level. Once a year, all Nachtwanderer meet to discuss their work and share experiences.

"Anwohnerinitiative Bremen" (Residential group, Bremen). The "Anwohner Initiative" is mentioned here because 2/3 of their members have taken part in a crime prevention measure run by a company called SelectaDNA. SelectaDNA is a marker spray with which one can mark property likely to be targeted in a burglary (i.e. jewellery, electronics, computers, furniture etc). The liquid is sprayed on property and it glows in UV light, enabling it to be traced back to the original owner if it is stolen. In addition to marking the items, members place stickers on the windows and building entrances to inform others that it is in use on the premises. Members chose to participate in this paticular initiative. This *Anwohnerinitiative* is part of a Germany-wide league of home owners, founded in 1919. The league is called *Verband Wohneigentum* e. V. (until: 2005: Deutscher Siedlerbund e. V. - Gesamtverband für Haus- und Wohneigentum) and is divided in local chapters, with membership ranging from only a hundred people to a few thousand. Membership is voluntary and its members are interested in a good neighbourhood, mutual help, autonomy and trust. For example. the local chapter in Bremen negotiated good oil rates for the annual oil purchase, as roughly 75 houses buying around 100,000 litres of oil (diesel) will get a good price per litre. Also, have they negotiated discounts in local DIY and gardening stores. Crime control and the SelecaDNA project is just one aspect of the work of this organization which is focused much broader issues associated with quality of life and community.

Neighbourhood watch in *Spain* is also heavily influenced by its authoritarian past. Spain has a long history of 'horizontal' surveillance. Social control and surveillance have been more the norm than the exception. In the 20th Century alone, Spain suffered almost 35 years of military rule (General Primo de Rivera between 1923 and 1930 and Francisco Franco Bahamonde, *El Generalísimo*, between 1939 and 1975), a Civil War (1936-1939) and several episodes of military upheaval in the first years of the Century. In the immediate post-civil war years after 1939 "All criminal activity committed in the national territory during the

red domination" had to be brought to the justice of the many special courts set up in order to organize the purging of reds, communists, separatists and freemasons.

While neighbourhood watch in Spain has never been a generalized or institutionally sanctioned phenomenon, ad hoc citizen patrols, which took law enforcement matters into their own hands, have emerged repeatedly since the end of the dictatorship in 1978. Due to changes in crime patterns, crime watch schemes in Spain have gone from cities to farmlands, from urban peripheries to rural and unpopulated areas. The first patrols appeared in the 80s and 90s in urban peripheries, mainly around Madrid, Barcelona and Valencia. Working-class neighbourhoods with large number of internal migrants that arrived from rural areas to larger cities looking for work formed the so called 'pickets of self-defence' [piquetes de autodefensa]. Neighbourhoods without many public services where citizens felt 'abandoned' by the Administration´s 'negligence'. These were also the areas where the heroin pandemic hit the hardest, and so trafficking, drug abuse and drug-related crime were common and for all to see. In the early 90s, 150,000 people were addicted to heroin in Spain, and in its worst period, the drug killed 300 people per year. Widespread drug addiction had a clear impact on community safety and people's perception of insecurity, with addicts consuming in public areas, stealing to buy drugs and suffering overdoses at people's doorsteps. The perceived lack of reaction by the authorities led some citizens to organize autonomously to patrol specific areas. With the development of Spanish democracy, services slowly arrived to these areas and, coinciding with a global trend, heroin consumption receded –and so did the citizen patrols.

In the late 90s and early 2000, neighbourhood patrols reappeared. This time, however, in slightly new scenarios –neighbourhoods with high rates of migrants from the Global South. The motivation for residents to self-organize to protect their areas was very similar to those of the 80s, namely to end drug dealing, prostitution, youth gangs and antisocial behaviour. But this time the migrants were not the actors but the 'deviant', the object of surveillance. We have identified such schemes in the neighbourhoods of Raval in Barcelona, Legazpi in

Madrid and in Mariana, in the city of Valencia. In the mid-2000s, urban patrols began to appear in rural areas and in residential developments of single-family homes or chalets, away from the urban centers, where public services are scarce. We have found these in the Alicante area, where residents organized themselves and formed patrols to protect their homes from theft. Especially since 2007, when the economic crisis started, farmers and ranchers began to be victims of larceny in their houses and farms. Their tools, electrical material, copper tubing, systems of irrigation, machinery, crops, diesel oil, livestock were being stolen and groups of farmers organized patrols, sometimes with the support of local authorities, in the areas of Lleida, Andalucía, Extremadura and Castilla.

In the exceptional case of the *UK*, Neighbourhood watch schemes, (or Home Watch schemes as they are sometimes referred to in parts of England and Wales), are active across all parts of the UK, which includes Scotland, England, Wales and Northern Ireland. Each nation of the UK has its own neighbourhood watch co-ordinating body, which registers the schemes. Schemes in their totality cover a significant section of the overall population, as statistics supplied by the British Crime Survey demonstrate. They estimated that, in 2006/07 '… 16 per cent of households currently belong to a Neighbourhood Watch scheme (this equates to an estimated 3.8m member households in England and Wales).[96] The reasons for creating (and the impetus for sustaining) these schemes can vary depending on localised and socio-demographic factors such as: the social classification and category of deprivation of the 'area'; levels of criminal activity; existence of the fear of crime; age of residents; religion of residents; relationships with the Police, and the levels of support being offered by other public sector agencies, such as local authorities, government departments or national neighbourhood watch support groups. Establishing accurate information on the number of active neighbourhood watch schemes in each country of the UK is a very difficult exercise to undertake, due to two principal reasons. Firstly, there is no single reliable source

[96] Nicholas, Siân, John Flatley (eds.) et al, Circumstances of Crime, Neighbourhood Watch Membership and Perceptions of Policing: Supplementary Volume 3 to Crime in England and Wales 2006/07: Findings from the 2006/07 British Crime Survey, Home Office, 2008.

of accurate information on the number of neighbourhood watch schemes in the UK. Secondly, information on numbers of schemes which is supplied from the national co-ordinating bodies for neighbourhood watch in the UK, i.e. Neighbourhood Watch Scotland; the Neighbourhood and Home Watch Network for England and Wales, and the Northern Ireland Policing Board (as representing the 3 Northern Ireland co-ordinating bodies), includes only those schemes which have been registered with these bodies, or the information has been supplied from studies which have been undertaken. However, there is evidence of the existence of a substantial and admittedly unquantifiable number of other 'live' schemes which have not been registered with the national co-ordinating bodies, but nevertheless have the same status, role and characteristics of schemes which are 'registered'. Schemes which have registered with the national co-ordinating bodies can receive information and guidance about starting up and fulfilling their role; advice on where to buy useful items such as signs and stickers, and can also register to receive national email alerts for dissemination on particular issues of safety relating to personal security, property, internet safety and for example keeping warm during the winter. It should be noted that schemes which have not been registered with the national co-ordinating bodies are not inferior to or have a lower status than schemes which have been registered. Schemes which are registered with the national co-ordinating bodies are more likely, than those which are not, to receive advice and assistance from the local police about their how to operate their neighbourhood watch scheme, and how to interact with the police. Laycock and Tilley provide evidence of the high number of schemes which were in existence in 1995:

> 'The growth of Neighbourhood Watch has been a crime prevention success story. There are now over 130,000 schemes in the United Kingdom all testifying to the commitment felt by the public to working with the police and other groups in controlling crime.'[97]

[97] Laycock, Gloria and Nick Tilley, Policing and Neighbourhood Watch: Strategic Issues, Home Office Police Research Group, 1995, p.12.

Nevertheless, the British Crime Survey 2009/10 reports that you are more likely to be a victim of crime if you live in one of the most deprived areas than if you live in one of the least deprived areas of England. Evidence from the Topping Report shows that there are far higher numbers of neighbourhood watch schemes in the least deprived areas than in the most deprived areas.[98] This is also the conclusion of the British Crime Survey in 2006/07: 'In general, the characteristics associated with lower levels of membership were those related to having a higher risk of crime'.[99] Bennett, in an earlier study also supports this view.[100] The relationship in recent years between crime figures and the establishment of neighbourhood watch schemes therefore appears to show an inverse relationship between areas with higher crime figures corresponding to fewer neighbourhood watch schemes being established. From the early 1980s to the late 1990s, the police took quite an active role in promoting neighbourhood watch as did many politicians, which undoubtedly had an impact on the growth of schemes, however this support has generally been diminishing across England and Wales, and Scotland, due to other priorities and diminishing resources. However, this is by no means a black and white picture, as 41 of the 43 police regions in England and Wales (from 2012) now have autonomous Police and Crime Commissioners who can respond to local needs and concerns. The position in Northern Ireland, where neighbourhood watch has been more actively promoted from around 2004, quite clearly shows a high level of ongoing police support for the establishment of neighbourhood watch across the province. The reasons for this may be more complicated due to the relatively recent establishment of a lasting political peace, and with the new Police Service Northern Ireland, which was established in 2002, maintaining its drive to develop stronger community safety links than perhaps could have been achieved prior to the Northern Ireland Peace Agreement. Surveillance practices used by neighbourhood watch schemes are not normally negotiated, or publicised, and do not tend to use surveillance technologies, and the balance of the

[98] Topping, John, Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake, 2012.
[99] Nicholas (2008) op cit.
[100] Bennett, Trevor, Themes and variations in neighbourhood watch, Crime, Policing And Place: Essays In Environmental Criminology, Routledge, 1992, pp.172-186.

surveillance power relationship therefore tends to lie with the neighbourhood watch members.

IV. 2 Stakeholders

The Stakeholders in Neighbourhood watch are depicted in figure IV.1. The stakeholders identified are amalgamated from the combined case studies. Stakeholders are divided into two groups: core stakeholders, the 'watcher' and 'watched' as we defined the original case study format and peripheral stakeholders. Core stakeholders in Neighbourhood Watch are all citizens who may be the subject of surveillance by neighbourhood watch 'schemes'. This includes suspicious persons and citizens who are critical of neighbourhood watch. Similarly citizens' property is a key target in the schemes. As discussed in the previous section, watchers are very diverse in character. They include neighbourhood watch volunteers who are sanctioned by official schemes, as well as police sponsored schemes, formal and informal community groups. In the diagram we have placed dotted lines between each of the watching stakeholders to indicate that there are tensions between them. In the following sections we will discuss how these tensions have emerged. Peripheral stakeholders are those who are not directly involved in watching or in being watched but who have engaged with neighbourhood watch more broadly. Typically peripheral stakeholders hail from a variety of institutional levels and include those who promote particular development and community safety strategies (including National and European governments), community safety and crime prevention charities, political organizations, mass who report on neighbourhood and social media which facilitates the sharing of information in schemes, residents associations and trading standards associations concerned with catching 'rogue' tradespeople.

IV. 3 Harms and controversies arising from NW

As with the other surveillance practices, Neighbourhood Watch-like arrangements are always instantiated to counter a particular harm or threat. Unlike the other surveillance practices covered in this report, the harm or threat is unspecified and can come from any

number of sources. Neighbourhood Watch schemes are set up to counteract feelings of insecurity, stemming from threats such as burglary and other property crime, the problems associated with drug dealing and addiction, anti social behaviour, prostitution and the presence of unfamiliar people and cultures in one's neighbourhood. Schemes also emerge after actual harms occur in relation to these threats, sometimes accompanied by media hype around a particular event. Frustration with the effectiveness of local police also causes schemes to emerge, sometimes around a single ring leader or entrepreneur who attempts to make a difference.

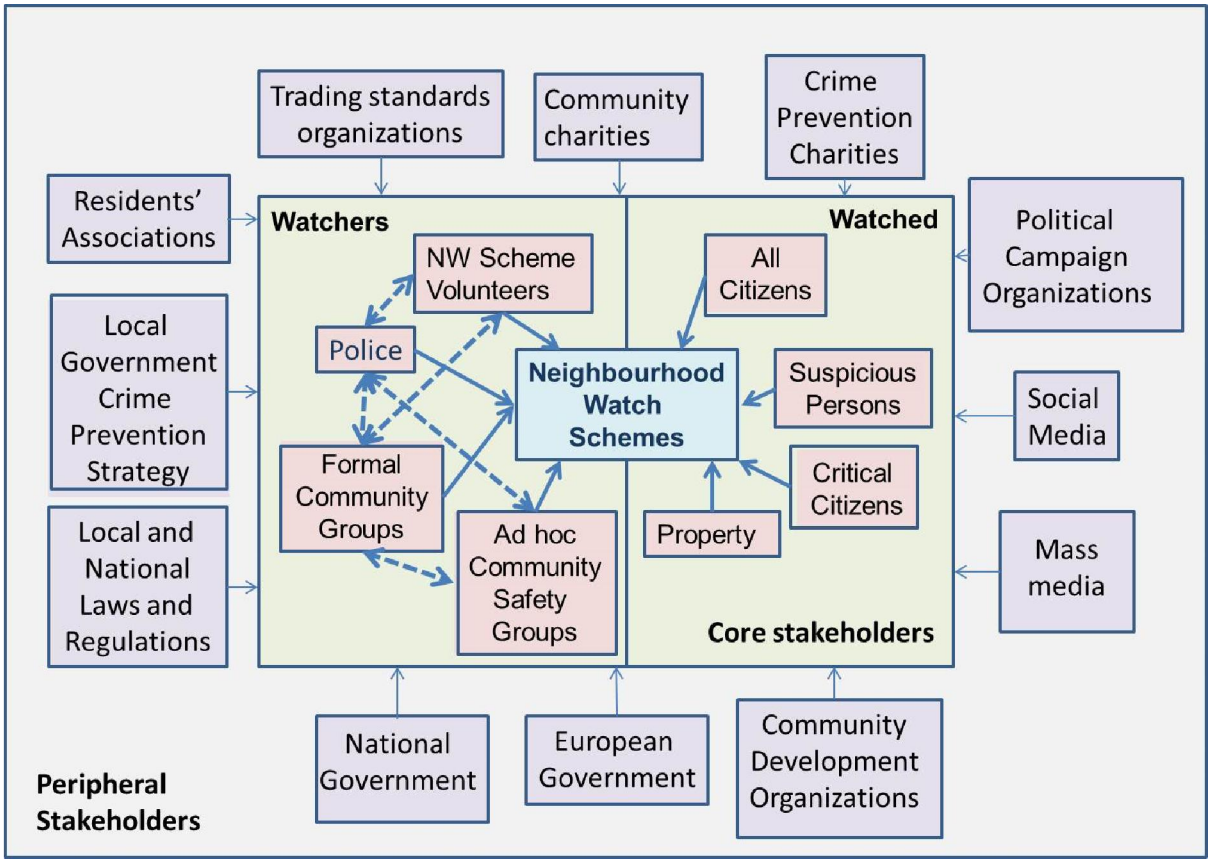


Figure IV.1: Neighbourhood Watch Stakeholders

And, in a manner similar to the other surveillance practices we have discussed, a number of harmful consequences arise from neighbourhood watch-style citizen-citizen surveillance. Using resilience terminology we categorise most of these harms as stresses and only one of them as shocks.

IV.3.1 Stresses

The stresses we discuss concern how neighbourhood watch can recharacterise a community, neighbourhood or place and establish new norms about criminality, suspicion and surveillance in that place. Neighbourhood watch schemes have the effect of stigmatising or re-stigmatising target groups who are already disadvantaged. Privacy has been seen to be infringed as information about targets is shared and surveillance becomes normalised. Watching out for suspicious behaviour in the community creates cultural acceptance of surveillance and a framing of the world as suspicious. One theme which underpins the whole discussion is the question of whether police are carrying out their roles as effectively as they might be. Tensions arise surrounding the remit of the police and whether communities can and should step in to manage their own safety.

Throughout Europe there has been a growth in the private security sector to extend, augment and replace state funded security agencies. The development and support of Neighbourhood Watch schemes is part of that phenomenon. The private security sector comprises a wide range of organisations which provide physical security services, technical sales, advice and training in military and civilian contexts. Its growth is attributed in no small degree to a number of pervasive national cultural, economic, political and social changes in recent years.[101] Recent theory has highlighted how the security landscape now comprises a series of interlinked nodes through which governance is achieved.[102] These nodes feature the aforementioned range of private security providers as well as government agencies, but Neighbourhood Watch extends the security landscape into the local community at a very low cost. Where the police's role is clear, such as in the UK or Germany, Neighbourhood Watch can be understood as a low cost extension to their community policing role. Debates do occur in these countries, however. By contrast in Austria and Spain there are greater frustrations and an avowed lack of police support for Neighbourhood Watch style

[101] See, Goold, B., Loader, I., & Thumala, A. (2010). Consuming security? Tools for a sociology of security consumption. *Theoretical criminology*, *14*(1), 3-30.
[102] Johnston, L., & Shearing, C. (2003). Governing security. *Explorations in Policing and Justice, London*.

interventions. In *Austria* Pro-Nachbarn is neither initiated nor actively supported by the police as an instrument of community policing. Police officials or local politicians think that neighbourhood watch schemes, addressing "crime problems" like burglary increase feelings of insecurity amongst the general public and therefore these activities receive some scepticism from public officials. Citizens are expected to report crime to the police but never get involved themselves. Similarly in S*pain* Neighbourhood Watch is illegal and the authorities were reluctant to accept parapolice schemes. In 2000, however, police in Cordoba and Barcelona began to take notice of the emergence of NW patrols if only as a barometer which indicated more policing was needed and that vigilantism needed to be tackled. Each of these stresses are now discussed in turn.

IV.3.1.1 Restigmatisation

The stigmatisation and restigmatisation of social groups and particular spaces is the first harm associated with Neighbourhood Watch – like schemes in the countries we investigated. In Austria, Germany and Spain, NW schemes have been used by right wing extremists and vigilante groups to propagate their beliefs about what is or is not an acceptable behaviour or even an identity in a particular area.

In *Austria* the municipal City Watch schemes were based on initiatives from local council members from right wing, populist parties. Playing on a toxic mix of fear of crime and xenophobia they launched campaigns against a presumed criminal group of migrants, blaming the police for not going effectively after the perpetrators. The issue was taken up by local media fuelling a heated debate about police incompetence, dangerous ethnic groups and the need to defend the citizens against threats linked to drug trafficking, public drinking, theft, pickpocketing, beggars, and crime in general. Along with the claim to establish City Watch as a form of public order policing there was a move to set up more CCTV in public space and to increase control of migrant populations. Despite available evidence and expert testimony to the contrary, city administrators finally gave in to the populist campaigns for

more security in public space. The main driver obviously were right wing parties promoting anti-migration, anti-crime, anti-disorder issues under the umbrella of setting up quasi-police forces. At the same time local media were more than happy to take up these controversial issues ("fear of crime sells") and police kept a low profile in the debate. On the one hand they accepted the claim of rising crime and disorder as problems to be addressed in one way or the other, but due to a lack of manpower and cutbacks in funding they pointed out they could not do more. On the other hand the police is the only institution who has the power of robust intervention, they can perform identity checks, arrest a person, ban individuals from certain areas – members of City Watch have to call the police and have no special powers or rights of intervention. Finally there were the pro-asylum, pro-migration groups voicing their concerns about racist ideologies, rising xenophobia and racist attitudes among the members of the City Watch teams. After initial phases of heated public debate the City Watch teams were established in the cities of Wels and Linz (and later on in a number of other cities like Graz). Up until now there is no independent evidence as to whether there has been an increase in perceived public security due to the new City Watch. Surveys conducted in Linz and Wels show mixed results so far and the police are reluctant to cooperate with these groups. Similarly in Berlin, *Germany*, the Sicherheitswacht was closed down after to two scandals, in which members of the Sicherheitswacht were involved. The first included racial discrimination and violent behaviour, and in the second it was revealed that members had a criminal record.

By contrast the *Wohnpartner* scheme managed to overcome ethnic stereotyping to create more positive outcomes for social housing residents in Vienna. Wohnpartner in Vienna was set up after a series of public complaints about daily conflicts in public housing estates. These conflicts were framed in the media as "cultural conflicts" among local residents and tenants from other ethnic backgrounds. Support came here also from right of the centre political parties. The main argument was that "foreigners" take over public housing originally meant to provide living space for the traditional Viennese population. With the establishment

of the Wohnpartner scheme the city administration managed to contain this controversy. The debate attracted a number of professional social work organisations, seeing an opportunity to get involved in a new field of intervention. Since the approach chosen by Wohnpartner was not narrowly confined to crime and disorder, they managed to avoid a stigmatising debate about crime and ethnic background. Activities comprise urban gardening, all kinds leisure activities, language courses and private lessons for students with learning problems. Hence Wohnpartner is not a Neighbour Watch scheme in the strictest sense, although it includes some elements of traditional NW.

Spain experienced significant problems with stigmatisation stemming from the vigilante basis of many of its informally organized 'citizen patrols'. Even when citizen patrols were intended to promote community safety, the impact of prejudice and racism on the way these schemes create the 'other' that needs to be watched is difficult to ignore. Also, as the neighbourhood watch schemes against drug use from the 80s show, even when integrated by working class people who rightfully feel that insecurity impacts their quality of life and that of their children by putting them at risk, it is always easier to chase a drug user than a drug dealer. Those watched and chased by patrol members are always the most vulnerable in their own ways – victims of a drug addiction, victims of people trafficking or exclusion in the case of prostitutes, and so on.

However, as is the case in Austria, there are also examples of neighbourhood watch-like schemes that defy this definition and explore the solidarity components of self-organizing to defend the community. As NW is informal in Spain and not sanctioned for any particular purposes, counter vigilante and community care groups also exist. In a middle-sized town in Catalunya, Reus, neighbourhood residents have organized themselves to help elders who have been attacked to go back to their normal lives by meeting them on a regular basis to go out in the streets and regain the confidence lost after an attack. Contrary to the examples mentioned so far, these groups do not seek media attention nor have specific demands to

make to the authorities. They see their schemes as a way to do the right thing and get involved in what happens in their neighbourhoods, and while some members do mention migration as a reason of recent neighbourhood decay, a racist discourse does not seem to have emerged from such initiatives.

Neighbourhood care schemes are not the only examples of neighbourhood watch that escape the link with vigilantism. In the Andalusian capital, Seville, several groups got together in the summer of 2011 to raise awareness on some situations which they felt were the result of the lack of policing, such as the growing number of informal 'parking attendants' that make a living by requesting a tip from drivers who want to leave their car in specific areas, or the shanty towns established in the outskirts of the city and inhabited mainly by people of a Romanian origin. These patrols were quickly dismissed by some of the more established neighbourhood associations and the authorities, and some radical organizations exposed the links between some of their members and the fascist far right.

As members of these patrols decided to gather regularly in different shanty towns and to harass parking attendants, some groups affiliated to the local radical left decided to organize 'contra-patrullas' and to meet at the same time and place as the members of the neighbourhood watch to force them to dismantle the scheme, with a degree of success, as the tweet written by a member of the counter-patrol and captured on February 23rd shows.[103]

According to a member of the counter-patrols, this initiative has managed to stop the 'racist' initiative by convening at the same time and place, but also by going to their assemblies and

[103] Xenophobic citizen patrol deactivated! Racists out of #Seville! #againstfascismnotonestepbackwards'

arguing against it, as part of a broader political effort to stop racism and fascism in the area. A similar development occurred in Madrid when activists felt some members of the central neighbourhood of Lavapiés were being harassed due to their looks and origin. This time, however, the profiling was not done by other citizens but by the police.

Police profiling is Spain is pervasive and illegal, according to several sources.[104] Stopping people to conduct identity checks based on the appearance of those who 'do not look Spanish' is a common procedure that has never been discouraged or punished by the police authorities, even if there is ample evidence that police profiling is discriminatory and racist. In 2011, after the 15M movement abandoned the squares to continue its activities at the local level, the neighbours of Lavapiés decided to make the struggle against 'racist police raids' one of their main activities, even if there have been campaigns dating back to 2008. Since then, videos of police operations stopping people of migrant 'appearance' are regularly posted online, and members of the community alert one another, via telephone, twitter and other means, when this happens, and they try to inform people about their rights, to disrupt the raid and expose the racist character of this practice. The members of these 'Neighbourhood Brigades to Observe Human Rights Compliance', who identify themselves with orange waistcoats, meet regularly to organize and coordinate their actions, and involve people of all ages who are usually politically active in the left and social movements at the local level.

According to their reports, between May 2010 and November 2012, members of the brigades recorded 1,144 racist raids, and their members have faced harassment and legal action, including criminal charges for obstruction and disobedience. These brigades are probably one of the most long-lived and active instance of neighbourhood watch in Spain, even if their activity is not what most expect when discussing neighbourhood watch schemes. These 'tales from the other side' expose a counterintuitive picture, where

[104] See, for instance: http://www.opensocietyfoundations.org/press-releases/report-un-details-pervasive-ethnic-profiling-spain

community organizing and surveillance are used to watch the watchers. Interestingly, it is in these 'other' patrols that we find greater diversity in terms of the age and origin of the participants, even if in some cases the political affiliations of members are relatively homogeneous.

IV.3.1.2 Privacy infringement

In each of the case study countries a rise in NW groups' use of social media to share information about their observations was noted. Boston citizens' use of Reddit following the Boston Marathon bombing illustrated how easy it was to mis-identify those allegedly involved in suspicious behaviour and for this process to get out of control[105]. The issue of privacy infringement has arisen particularly in Austria, as Pro-Neighbour has made extensive use of social media in its activities and began to create a database about its observations which it attempted to share with police, who were not interested. The database contained speculative personal details of those they had observed, which the police erroneously turned down on data protection grounds.

Pro neighbour's internet use runs from its blog, through to its Facebook page, forum and You Tube channel. On the blog, registered users can report incidents and make them public via this website. An example of an entry is*: I've heard a noise and saw a white box-type lorry with a Eastern-European number plate parking in front of my house, what shall I do now?"*. On Facebook users are discussing various incidents that have occurred. Whilst on Facebook the discussion is rather distinctive, the openly accessible and anonymous Internet forum of Pro-neighbour offers a platform to discuss concrete incidents as well as share more general thoughts on crime prevention. Finally its YouTube channel documents Pro Neighbour appearances on local (Austrian) TV stations.[106] The effectiveness of neighbourhood watch schemes as a compliment to police work always has media coverage when burglary rates

[105] http://www.usatoday.com/story/news/2013/04/25/boston-bombing-social-media-student-brown-university-reddit/2112309/ accessed 20th May 2014
[106] See, http://www.youtube.com/user/pronachbar.

are increasing (before Christmas and the summer holidays) and Pro Neighbour seem to always be ready to appear in the media.

In *Spain*, the use of social media by NW groups raises privacy concerns because images of specific individuals (personal data) are or will be circulated without permission, consent or registry. For example, In 2010 an English-speaking Barcelona resident launched a website and Facebook page called 'Robbed in Barcelona' in order to 'raise awareness of the situation in Barcelona, but more so to embarrass the local authorities into action'.[107] The site encourages people to anonymously send pictures, videos and tips on pickpockets and thieves in Barcelona, and there are frequent stories of robberies detailing methods and the physical appearance of those identified as perpetrators. While some comments are just descriptions or laments for things that have happened, others tell stories that are quite hard to believe:

But foreign residents are not the only ones to use ICT in this context. In 2013 a so-called 'somatén' in a town of 2,000 people, Riudellots de la Selva, launched a Facebook group and a 'whatsapp' account that members use to exchange tips and pictures of any abnormal activity they spot. The contributions are a mixture of self-promotion, dissemination of relevant news pieces, comments about specific crimes that occur and stories about people begging, looking for a place to squat or just wandering around in the village. The information that is shared does not seem to be a contribution to an offline dynamic, but a fully online experience which may or may not translate into a 'physical' scheme if the community experiences an episode of stress related to security.

[107] See http://www.robbedinbarcelona.com/2010/03/09/the-creation-of-robbed-in-barcelona/

Finally, as mentioned above, a regional paper recently reported that some rural neighbourhood watch schemes are planning to use unmanned aerial vehicles equipped with high-resolution thermal imaging cameras and night vision. While the wording of the news piece revealed that this is just the vision of the company trying to sell the drones to members, it is quite likely that this will become a reality in the near future.

In the *UK n*ew social media is being used for communication purposes, but from national co-ordinating bodies to local groups. It is sometimes used locally to 'out' or 'publicise' the activities of suspicious local people. The 'Neighbourhood Alert' system, used by the national co-ordinating bodies has changed communication patterns from the disjointed arrangements which were used previously. Having said that, many schemes are not registered with the national co-ordinating bodies and therefore miss out on communications alerts, while others may miss out due to lack of either internet access or technical ability to use the internet. According to the Neighbourhood and Home Watch Network, 'Neighbourhood Alerts' often feature in news and other media. Surveillance practices undertaken by neighbourhood watch volunteers do not tend to use surveillance technologies, but communication methods by national neighbourhood watch co-ordinating bodies and neighbourhood watch groups locally, use new social media technologies extensively.

IV.3.1.3 Normalisation of surveillance

The sheer prevalence and formalisation of NW schemes in the *UK*, alongside other aspects of British society (for example the extent of its CCTV use) raise the question as to whether surveillance practices are becoming as normal in community relations as they are in arenas such as policing. This case study questions as to whether it is becoming culturally acceptable in UK to surveil one's neighbourhood and to identify suspicious behaviour, vehicles or other objects at every turn. One is reminded of the London Metropolitan police's 'If you suspect it, report it' campaign which implored London residents to report anything

they considered suspicious to the police (people, houses, cars etc)[108]. New policing rules also outlawed photography in important public places, of important buildings, infrastructural or CCTV installations to the extent that tourists were constantly challenged by police in London[109]. Being subject to and exercising surveillance is becoming culturally normal in Britain. Neighbourhood Watch schemes have extended to other forms of 'watch' activities which are closely linked to many other initiatives which promote and support personal and community safety, such as Community Speedwatch (targeting roads which are deemed to have problems with speeding motorists); Shopwatch (where information on known offenders such as shoplifters is shared); Horsewatch; Farm Watch, and Pubwatch (where information on known troublemakers, including sometimes their photographs, is shared amongst licensed premises).

Despite this increase in local surveillance in all manner of situations in some parts of the UK there has been a change in focus for such programmes. In Scotland, for example, there has been a discernible change from neighbourhood watch activities being centred on 'soft' surveillance and the monitoring and reporting of suspicious activity and movements, to a more inclusive and caring approach in which improving the safety of communities features strongly. This involves for example, giving advice about online security, bogus caller alert schemes, semi-formal arrangements for sharing of holiday information with neighbours, and generally making vulnerable people feel safer. An example of this move towards a more humanitarian role can be found on the Neighbourhood Watch Scotland website which offers the following examples of how to care for neighbours and family members:

- *'In previous years, severe weather left some people vulnerable. Helping each other a little can make a big difference. Here's how you can play your part in making your community more prepared:*

[108] http://content.met.police.uk/Campaign/nationwidecounterterrorism accessed 20th May 2014
[109] http://photographernotaterrorist.org/ accessed 20th May 2014

- *Identify family members or neighbours who may need an extra helping hand if severe weather strikes*
- *Have their phone numbers to hand*
- *Offer to help with grocery shopping or other essential tasks*
- *Clear ice or snow from pathways*
- *Volunteer to help others by visiting www.volunteerscotland.org.uk*
- *If you are part of a community group, think about what your group can do to help others during bad weather'*

While the UK moves towards a surveillance society, neighbourhood watch schemes extend and care discourses are mobilised the opposite is true in *Germany.* There, surveillance measures of any kind are always discussed in relation to its totalitarian regimes of the 20th century. Especially crucial is the connection between official and non-official surveyors - the genuine "totalitarian" aspect. Without any exaggeration, one could say that this experience of surveillance has been a shock to the system of values and norms within German society, which can still be traced in a repertoire of interpretative routines, symbols and expressions circulating today.

Discussions on introducing "neighbourhood watch schemes" in Germany in the early 1990s (which were finally rejected), were countered with arguments referring to "Bayern-Stasi", and "informership"/grasses, "…that have its predecessors in the Blockwart." This is partly why the "Sicherheitswacht" – emerged, to counter these accusations. It was said:

> *"The Sicherheitswacht is no auxiliary police. It should not replace but complement the work of the police. Also it is no "Bürgerwehr" (i.e. an uncontrolled association of*

citizens who believe they must take care of law and order themselves. The Sicherheitswacht is the better and constitutional alternative."[110]

Therefore, an organized and active way of surveilling the neighbourhood in general can be considered as a "no-go": "Wachsame Nachbarn" is about being watchful of suspicious behaviour by strangers that one can see from one's window, not about patrolling and looking at everybody. Again, the Nachtwanderer organisation is about young people at night, not about having a look at anybody in any place. Thus, to establish some form of "citizen to citizen"-surveillance, one has to specify a certain mutual, one could say "dyadic" relationship between the watchers and the watched (door-to-door neighbours, parents/kids). Only the "Kiezläufer" organisation adresses "people in general". However, these are not randomly recruited amateurs, but "professionals" in a way that they have to pass some education before they are allowed to do their job. They have an institutional context, in which they are monitored themselves.

Some interviews showed that "neighbourhood watch" as a term constitutes a closed discourse, (an insular debate) which has no or rather irrational connections to other beliefs and opinions. I.e., people might be worried about the situation in their neighbourhood, they might hope for "something to happen" and might also be sceptical about the police, but still refuse "neighbourhood watch" as an means to get what they want, as this interviewee describes:

Yes that is happening. Here in these houses everybody cares for each other. Even with the changes going on, even when foreigners move in here. But when they are well integrated into the Germans, they take part. Well everybody has its own little spleen. But when there is somebody strange, then he or she will be approached. And

[110] SCHMIECHEN-ACKERMANN, DETLEF (2000)„DER „BLOCKWART" -Die unteren Parteifunktionäre im nationalsozialistischen Terror- und Überwachungsapparat", in: Vierteljahrshefte für Zeitgeschichte, Vol 48 (4), p 575-602.

someone will notify you: ‚I have seen someone in your garden. Be careful'. And we did not have problems. But you cannot force this. This is grown over years and decades. And this is a problem, too. Try to integrate the new owners or tenants into this structure, that is not easy.

The interviewee partner stresses mutual help among neighbours, but nothing more than that. The key to understanding this is the remark about the depth of the relationships that have grown over years that are the basis for such mutual help. A woman from the same estate states this quite distinctively. When questioned about the "Alert Neighbour" sign near her house, she said:

It works with the neighbours. We talk about what is happening, especially with the woman from the one side. She tells me then, ‚there have been strange people here, setting up boxes to collect used clothing. She watches out, she knows when I am not here, and then she just has a look at it.

When she was asked about neighbourhood watch schemes, her tone changed:

Some people are nuts. I think that is totally useless. When people live together, and I mean not only sharing estates or houses, but living, nobody has a chance to intrude. That's what it's all about. It's the relationships, that has to work. If that is not working, then you can have someone with a rifle patrolling and it is of no use what so ever. If people have the feeling they have to defend themselves, they have made the step far too late. They have to talk to each other. I think of it from the side of the community (Gemeinschaft).

Nevertheless the gap between individual and institutional responsibilities – once filled by community activities - is mentioned every once in a while. So the "alienation between the work of the police and the citizens" was a key factor in preparing the introduction of the

“Sicherheitswacht”; there are also many efforts to establish community life and to address and enforce collective responsibilities.

In summary, stresses around neighbourhood watch concern debates over the proper remit of the police, the restigmatisation of a place, particularly through racism and vigilantism, privacy, as NW schemes increase their use of social media and the normalisation of surveillance. However these stresses are not universal in that they do not occur in all of the cases. Neighbourhood Watch, by its nature, is community based and is thus subject to constant re-negotiation and re-interpretation by its stakeholders. In turn the meaning of neighbourhood watch is heavily rooted in a community’s history and culture, the historical nature of authority relations between police and community, and the role of the police, police effectiveness and the character of governmentality in respect of law and order.

IV.3.2 Shocks

Both Germany and Spain have experienced shocks because of the actions of NW-type groups. In *Germany*, any positive action by a NW group is an extremely sensitive issue Only recently in September 2013, there has been controversy surrounding a young neighbourhood watch organisation in Würzburg/Bavaria. In December 2012, a 23 year paramedic founded the “Einsatzgruppe Lupus”, an organisation of about 20 citizens. Its members were employees of the emergency services. They patrolled the city of Würzburg, trying to settle disputes among drunken people, prevent vandalism committed by young people and so on. They wore uniforms which had a wolf as its logo (lupus) and a number so that they could be identified in case of controversy. The group chose to equip itself with tools such as torches, hand-cuffs and pepper spray. They reported their actions on their Facebook-page, where they also posted pictures of incidents and appealed for help in finding suspicious people. They also had a YouTube channel to promote their work. When patrolling they communicated with each other via an app-based radio-handset “Zello”, which

recorded their communications and made them available for the public as podcasts. So they worked in a very transparent way and tried to be as inclusive as possible.

In an incident in early September one of the members made use of the pepper spray, which attracted the attention of the media and the police. Since then, the work of Einsatzgruppe Lupus has been debated widely in the local media. Again we can observe, how deeply shocking it is if a neighbourhood watch group takes any kind of action. The accusations of "being a Bürgerwehr with right-wing tendencies and vigilante justice", "of being secret Blockwarts, that nobody wants" is on their facebook page.[111] The police have supported these arguments and have demanded stronger control of this group by the local government: "Since they lack any experience and education to act in such a sensitive fields, which endangers them as well the persons they confront." [112] The police are also concerned that the organisation might inspire other people to act in the same way. For the moment the organization are no longer allowed to wear uniforms, have handcuffs and to carry pepper spray with them. They cannot be legally banned but they are now subject to intensive scrutiny themselves.

The situation feared by the German police has been a reality in *Spain* for some years. It is particularly shocking that urban vigilante 'patrols' have routinely resorted to violence to rid their areas of what they perceive as threats. For example, In 1991 there were four 'patrullas' in Barcelona's metropolitan area (Barcelona, El Prat, Badalona and Sant Adrià) that chased drug addicts and dealers to literally beat them up and kick them out of their neighbourhoods. While different kinds of patrols appeared in places as diverse as Sagunto, Palma de Mallorca, Valencia, Alicante, Madrid, Almería, Cartagena, Huelva and Pontevedra, in most places the community response to the problem were peaceful demonstrations and meetings with the authorities. In places like Móstoles, San Blas, Alcorcón, Valencia and El Prat,

[111] https://www.facebook.com/einsatzgruppe.lupus
[112] http://www.mainpost.de/regional/wuerzburg/lupus_w%FCrzburg_2013.artikel/Stadt-erlaesst-Verbote-gegen-Nachbarschaftswache;art735,7701980

however, there were reported instances of attempted lynching, with members of the neighbourhood watch walking around with 'sticks, chains and umbrellas', stopping busses to kick out the drug users and, in one case, chasing a drug addict up into a building and threatening to throw him off. There were also instances of fascist-like bands joining the neighbourhood patrols, which were a combination of poverty, prejudice and racism (most drug dealers were said to be Spanish Roma). The police stepped in and all authorities spoke out against neighbourhood watch schemes, and were convinced that the police was the only body that could face the problem properly and within the limits of the law. In 1992 Spain passed its first Community Safety law, giving the police increased powers and establishing new, harsher fines for drug use in public places.

While the Spanish authorities reacted to NW based violence in the 1990s, the problem has arisen again in response to different types of perceived threat, such as migrants and rural crime. Bearing this in mind, we now turn our attention to the broader questions concerning governance of neighbourhood watch, and other democratic encounters which might limit its harms and enable communities to be built in the most appropriate way.

IV. 4 Democratic encounters with NW

In this section we discuss the extent to which neighbourhood watch schemes intersect with democratic processes and are subject to internal scrutiny. In Austria, Germany and Spain we find low levels of intersection in all categories as NW schemes tend to be outside the formal governance structures relating to law, order and community safety and have been set up on an ad hoc basis. In the UK, there is widespread engagement with and awareness of NW, but loose governance and participation. We consider each of these categories in turn.

IV.4.1 Governance

In *Austria* there is no legal reference to NW type schemes in relation to crime and policing. The Security Police Act (Sicherheitspolizeigesetz – öSPG) states that only the Police are

entitled to investigate crimes, pursue suspects and perform stop and search activities. Private security companies or neighbourhood watch schemes are not allowed to stop citizens and to perform identify verifications as the Police can do. The activities of Pro Neighbour as a non-profit association are regulated by the Austrian Associations Act 2002 (Vereinsgesetz 2002). Because Pro-Neighbour is organised as a non-profit association it is not entitled to receive any public funding. The membership is free, although donations and sponsors are welcome.

Furthermore, the Austrian Ministry for Interior has no general policy or guidelines on how local police should cooperate with initiatives such as Pro-Nachbarn (P-N). One such area where P-N has attempted to co-operate with the police is through the sharing of data on their observations. It has also attempted to extract crime data from the police to further refine their own activities. While organizations such as P-N like to collect data on their observations, the police have a strict and restrictive policy with regard to crime data. No data are made available beyond the annually published crime statistics. While local initiatives would like to have more information the police does not grant access to such intelligence.

Similarly in *Germany* there is a low incidence of neighbourhood watch because there is a strong cultural tradition of compliance with authority and a fear of community groups taking matters into their own hands. Only the *Sicherheitswacht* – the volunteer police force, is accountable to the police, government and the public as it is an official extension of the police and hence subject to some of their governance mechanisms. Other informal NW-type organizations attempt to maintain their own levels of transparency and accountability and volunteer share information with local government and police. The *Kiezläufer,* for example, gather their own statistics about the number of times they speak to groups of young people and single young people. They also record the number of incidents they have referred to law enforcement, the number of times they are called by citizens and institutions and the number

of times they have intervened in an incident. Local government gather these statistics which are then discussed with the police to decide whether the schemes themselves continue. Furthermore, the media also report on these statistics. Other, less formal organizations such as *Nachtwanderer,* who are not supported or sanctioned by any official institution do not report their activities anywhere and their work is not monitored at any official level.

The situation is *Spain* is even less formal than in Germany or Austria. The state firefights on particular issues following particularly notorious crimes or other events but has no coherent policy or approach to local groups interested in community safety. The media plays a strong role in influencing public opinion. The promotion of community safety is formally assigned to police and other security forces. The 1978 Spanish Constitution establishes that 'The Security Forces, subordinated to the Government, will have as their mission to protect the free exercise of rights and liberties and to guarantee community safety' (Art. 104).[113] The Organic Law that regulates the Security Forces (LOFCSE 2/86) establishes that it is the State and its institutions, at its different levels, that is responsible for maintaining public security, and underscores that this is an exclusive competence reserved to the state and its institutions. The only exception to this monopoly is found in municipalities where there is no local police. In such cases, the duties of the police will be fulfilled by 'personnel working to guard and surveil goods, services and buildings' such as 'guards, watchmen, officers, bailiffs or similar' (Art. 51.2).[114] This opens the possibility for local authorities to hire citizens or private security officers to work on security matters at the municipal level. Similarly, the State's monopoly over public security cannot stop citizens from guarding their property or reporting crimes to the police. Article 259 of the Criminal Procedure Code established that it is mandatory for individuals to report any crime they may have been witness to, to a judge.

Therefore, while neighbourhood watch schemes are not regulated in Spain, if their only function is to surveil and alert the police when necessary, they are not forbidden. However,

[113]http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingles_0.pdf
[114] ibid

their members cannot be recognized as a public authority and if they used force or tried to hold someone they could be charged with several offences, such as illegal detention (Art. 163.4 of the Penal Code). As for legitimate defence, Spanish law only considers it as an exception of the penal responsibilities one may have if the following requirements concur – that there is an illegitimate attack, that there is a rational need for the use of the means chosen to stop it or repel it, and the absence of a sufficient provocation on the part of the person defending him or herself.

The fact that such schemes have never been legal has meant that the landscape of neighbourhood watch in Spain is significantly different to that in other European countries. Not only because it is not a generalized or institutionalized phenomenon, but also because when it has arisen, it has done so in very different ways. The absence of a 'template' or 'model' that citizens can replicate has resulted in citizen patrols taking unexpected forms, and neighbours organizing against crime, but also against the police and even against other neighbourhood watch schemes.

In the *UK*, neighbourhood watch schemes have national co-ordinating bodies, with which they can register. National co-ordinating bodies give advice on how to establish a scheme which includes provision of a draft constitution, although it is not known how many schemes actually adopt a constitution and then comply with its requirements. To that extent, neighbourhood watch schemes can be regarded as self-regulating. The fact that neighbourhood watch scheme members are unelected and volunteers, does call into question the legitimacy and representativeness of their 'voice', however there is undoubted widespread support for their activities, and participation in neighbourhood watch activities is a commendable form of active citizenship and members should be recognised for the contribution which they make to the safety of their community.

When schemes register they receive information and guidance about starting up and fulfilling their role; advice on where to buy useful items such as signs and stickers, and they can also

register to receive national email alerts for dissemination on particular issues of safety relating to personal security, property, internet safety and for example keeping warm during the winter. Schemes which are registered with the national co-ordinating bodies (and there are some which are not) are more likely to receive advice and assistance from the local police about their how to operate their neighbourhood watch scheme, and how to interact with the police.

National co-ordination of neighbourhood watch activities in Scotland commenced in 2006 with the Association of Scottish Neighbourhood watches, which subsequently changed its name to Neighbourhood Watch Scotland in 2011. It is registered as a Scottish Charitable Incorporated Organisation. It employs 2 members of staff and is governed by a Board of Volunteer Trustees, with funding being provided by the Scottish Government. One of its key objectives is: 'to help people work together to make their communities safer.'[115] It is very difficult to know exactly how many schemes are active at any one time. This fact is exemplified by Fyfe who records that in 1996/97 within the Strathclyde Police force area alone, there were 1,671 schemes, and 4,597 within Scotland, although by 2005/06, there were 427 schemes within Strathclyde and 2,874 within Scotland. Fyfe ascribes the growth in interest in neighbourhood watch to government policies in the 1990s which promoted active citizenship, and 'civilian policing' which took the form primarily of neighbourhood watch and special constables (volunteer police). The Association of Chief Police Officers in Scotland (ACPOS) also acknowledges the work of special constables and community wardens in assisting community police officers: 'The targeted use of the Special Constabulary, volunteers and community wardens will provide resilience and support the work undertaken by community police officers.'[116]

[115] Neighbourhood Watch Scotland: http://www.neighbourhoodwatchscotland.co.uk/pages/1363/1/What_is_Neighbourhood_Watch_Scotland_.html

[116] ACPOS Public Reassurance Strategy: http://www.sipr.ac.uk/downloads/ACPOS_Public_Reassurance_Strategy_310707.pdf

Community police officers and special constables are the link between neighbourhood watch and the police in England and Wales as well. Neighbourhood Watch in England and Wales was originally called Home Watch, a name by which it is still known in some parts of the country. In 2007, with support from the Home Office, the Neighbourhood and Home Watch Network (England & Wales) was formed. Prior to this, there had been a national co-ordinating body for England and Wales called the UK Neighbourhood Watch Trust, however this was disbanded due to internal and irreconcilable differences amongst some of the members and co-ordinators. This may explain why some current members and co-ordinators of neighbourhood watch schemes are unwilling to register with the national database, or to become involved with national initiatives. For example, in Wales there is some active opposition by their members and coordinators to the national database, and as a result, fewer schemes have registered than are known to exist. The Neighbourhood and Home Watch Network currently have seven employees, and provide support to new groups wishing to start-up, including directing people towards the various resources on their website, such as Toolkits, a Document Library, and a Members Area. Local Associations may provide further and more detailed support depending on the characteristics of the area, what the local issues are, and what the relationships are like between the local Neighbourhood Watch groups and the police.

The introduction of elected Police and Crime Commissioners in 2011 has changed the landscape again. These new commissioners replaced older ‘police authorities’ throughout England and Wales and are set up to hold police chiefs to account and to represent the people’s views on policing. Police and Crime Commissioners are directly accountable to the public and have the democratic mandate to respond to local people’s concerns. They can also have some say in policing budgets and can work with local partners to prevent crime. They work with local and county councils to improve policing and specifically promote neighbourhood watch as a community building and crime prevention strategy.

The situation in Northern Ireland is slightly different due to emerging political stability and the peace process. Police take a more active role in neighbourhood watch than in the rest of the country. Overall co-ordination of neighbourhood watch in Northern Ireland is undertaken by a steering group involving representatives of three organisations, whose details and purpose are described as follows:

> '*The aim of Neighbourhood Watch is to support you so that you can protect yourself and your property. The scheme is promoted, supported and endorsed at a strategic level by a partnership (Steering Group) comprising representatives of the Department of Justice, the Police Service of Northern Ireland (PSNI) and the Northern Ireland Policing Board (NIPB). At an operational level, this is done through PSNI District Command Units and Policing and Community Safety Partnerships.'* [117]

Whilst the distribution of neighbourhood watch in Northern Ireland mirrored that in the rest of the UK – in that the majority of schemes are in the least deprived areas whereas crime occurs in the most deprived areas - there is a unique socio-demographic factor, that of religion. The vast of NW members are Protestants as opposed to Catholics. The Northern Ireland Peace Agreement which was concluded in 1998, set the ground for peaceful civil relations to be established between the unionist and nationalist communities, and there has been sustained growth in the numbers and coverage of schemes in the last decade.

IV.4.2 Participation

Neighbourhood watch, perhaps unsurprisingly, experiences very low degrees of stakeholder involvement and participation beyond interested and participating citizens and the police. The quality of interaction with the police varies to a very great extent.

In *Austria*, The main stakeholders include the media, police, activists, political parties, and local communities. The police do not like NBW or other groups such as citizen patrols or

[117] NI Direct, Northern Ireland Government's website: http://www.nidirect.gov.uk/neighbourhood-watch accessed 27th May 2014

vigilantes being formed, but they do want to have access to citizens. The media often acts in its own self-interest, i.e. if a story is spectacular, for example about a particularly scandalous crime, it will sell papers. there is very low cooperation with the police around community safety altogether. In fact this lack of co-operation and perceived ineffectiveness of policing in public space and in relation to domestic crimes (such as burglary) is frustrating for citizens and often sparks them into forming NW-like schemes. This problem of perceived 'insecurity' emerged from local media hype, but the figures for recorded crimes are extremely low. The participation which does occur is between NW schemes and other schemes throughout Europe. Pro-Neighbour is regularly present at several national "security related events" such as crime prevention days or neighbourhood fairs. 2011 Pro-Neighbour visited the UK and signed a Memorandum of Understanding with a British Neighbourhood Watch and Home Watch Network. Since 2009 Pro-Neighbour is listed in the EUCPN (European Crime Prevention Network) as a good practice example for crime prevention and Pro-Neighbour was awarded a European Crime Prevention Award in 2012. In 2013 the SELPE Project (Sharing Experiences in Local Policing in Europe) took note of Pro-Neighbour and invited representatives from the Association to several project workshops.

In *Germany,* the police actively oppose NW and politicians rarely vote for it. The appeal is for individuals to do things unilaterally, but not to organise themselves as a group. The independent NW schemes therefore form their own networks. *Anwohnerinitiative Bremen* formed its own relationship with SelectaDNA to participate in a 'smart water' scheme. The *Kiezlaufer* initiative Hamburg worked with youth groups, an institute for mediation (IKM) and with local councils. As with Pro-Nachbarn in Austria, Nachtwanderer has a national conference where information and tips are shared. The media, as a peripheral stakeholder has a major role to play in limiting the activites of informal NW schemes, reproducing discourses about right wing extremists and left wing vigilantes ever time the issue is publicly debated.

In *Spain*, because of the total lack of police or local authority interest, the meaning and practice of NW is constantly re-determined by its stakeholders. The media often set the agenda by raising awareness and the police tend to react to community demands to deploy more resources on an ad hoc basis. Individual 'patrols' have made attempts to speak to local councils about their needs, but this has never been formally acknowledge. On only one occasion was a patrol given funding and a meeting space in Tarragona in the mid-1990s. NW will never be a politically acceptable solution in Spain.

In the *UK* the picture is a little more formal. Scottish, Northern Irish and UK Governments fund the respective national co-ordinating bodies for Scotland, N. Ireland and England and Wales. This funding is for staff costs and offices, with little remaining for media campaigns or starter packs for new groups. NW is very much a 'bottom-up' grass roots activity which is self-regulating, and generally free from political interference. Close links will commonly be developed with many other groups and the authorities – notably the police, local authority, and local councillors. At the outset of NW in the UK in the 1990s it was promoted by the UK government and the police, but there is little political involvement now and the role of the police has generally been revised to one of lesser involvement. This is due to competing priorities and diminishing resources. In Northern Ireland there is strong police engagement with NW, and in England and Wales there has been a recent change involving the de-centralisation of decision making on police matters to 44 area Police and Crime Commissioners, discussed in the previous section.

Since the inception of the first neighbourhood watch schemes in the UK in the early to mid-1980s, the police have had a major influence on the growth, sustainability and diversity of interests of neighbourhood watch schemes. The police can rightly be attributed to having engendered resilience within communities by encouraging them to form neighbourhood

watch schemes. Police in the UK according to Bolton[118] were responsible for promoting neighbourhood watch as a form of active citizenship to reduce the costs of policing. Fyfe[119] and Henry[120] however, attribute successive governmental policies as being responsible for promoting the growth of neighbourhood watch as part of the drive to increase the development and reach of community policing. McConville and Shepherd[121] also expand on the rhetorical support provided for neighbourhood watch by politicians, including those at governmental level. The role of politicians and governments in directing the activities of the police is an important one, and undoubtedly has had a major influence on the relationship between the police and neighbourhood watch. The Scottish Government for example created 15 national outcomes, one of which is 'we live our lives safe from crime, disorder and danger', and one of the 5 national strategic objectives is to make Scotland 'safer and stronger' with an emphasis on community safety. Part of the approach in Scotland to resolving problems of crime and fear of crime (along with many other societal problems such as youth unemployment, and anti-social behaviour), has been to use partnership working, legislative provision for which has been made through the creation of community plans, involving all of the public sector organisations, including the police, within a community plan area working together to solve these types of problems, which are often inter-related. Donnelly[122] also refers to the increasing role which Community Wardens are now playing, many aspects of which were formerly fulfilled by Community Police Officers (CPOs).

IV.4.3 Engagement

As is the case with stakeholder participation, public engagement with Neighbourhood Watch is low in Austria, Germany and Spain and reasonably high in the UK. It has emerged that

[118] Bolton, Sharon, Crime prevention in the community: The case of Neighbourhood Watch, Taylor & Francis, 2006, p.40.
[119] Fyfe, Nicholas R., Policing Crime and Disorder, in Policing Scotland, Daniel Donnelly and Kenneth Scott (eds.), Wilan, 2013, p.190.
[120] Henry, Alistair, The development of community safety in Scotland: a different path? Crime prevention policies in comparative perspective, Willan Publishing, 2009, pp.86-109.
[121] McConville, Mike, and Dan Shepherd, Watching police, watching communities, Routledge, 2013.
[122] Donnelly, Daniel, Community Wardens in Scotland: Practitioners' Views, The Howard Journal of Criminal Justice, Wiley Online Library, 47, 4, 2008, pp.371-382.

media coverage is particularly powerful way of mobilising debates about NW in the former three countries as it is often sensationalised in particular ways. In the UK, where NW is normal, little media coverage has been found – it more likely to be parodied in British popular culture than sensationalised in the press.

In *Austria* there is very little widespread public engagement with NW. Austria is one of the safest countries in which to live. In Linz and Wels where there are City Watch schemes, left wing politicians have encouraged public monitoring and criticism of City Watch officials (who are paid by the Government), but in reality there is no underlying crime problem. Neighbourhood watch schemes in Austria face the problem in public's perception crime is an issue to be addressed by the police and not by citizens. Neighbourhood watch schemes emerge in districts or areas with a high proportion of houses/apartments that are owned by the residents. In central districts of Vienna or other larger cities where most of the apartments are rented or are part of a block of council flats hardly find any active neighbourhood watch schemes are found. The few neighbourhood watch schemes in Austria as observed and described in this report have a strong community aspect. Neighbours looking after each other, do the grocery shopping when someone is sick, share their private pools or the saunas, organise barbecue parties for the neighbourhood during summer times and so on. Interestingly, from the approximately 15 members of neighbourhood watch schemes in Austria interviewed for this report, no one was below the age of 40, all them reported that it is very hard for the scheme to get young people or young families involved in their activities.

Pro-Neighbour now has approx. 6,000 registered users/members. Not all of them are active "neighbourhood watchers" but all have access to the reports the network provides through its mailing list. Although its website was initially focused on issues in the immediate neighbourhood, the initiative later on developed into a communication platform for its members. Interested citizens can register online and receive information about incidents in the district they are living. Pro-Neighbour actively engages with the media and it appears to

have two strategies. Sometimes they tend to give provocative statements, announcing that their members will start to wear uniforms and run patrols on the street level as the police are ineffective. Currently, Pro-Neighbour are neither uniformed nor they are patrolling their neighbourhood. On other occasions they emphasise in their media statements that they are willing to cooperate with the police and that communication about crime is the best preventative measure.

In *Germany* public engagement with any informally organized NW schemes are to counter the practice. The police and the public sometimes combine their arguments to criticise any right wing tendencies which might be motivating people to engage. Reports about domestic „neighbourhood watch schemes“ in the media are never really focussed on a well observed, currently ongoing practice, but are analysed with respect to the historical experience of vigilantism in Germany. NW are always a sensitive issue. At best, they report about the latest developments for example the “Sicherheitswacht”, in 1992. The federal government proposed the idea and thence followed a political discussion which attempted to identify whether it was the most appropriate response to several problems: rising crime, burglary, the rising cost of policing, alienation between police and citizens, and a lack of community within neighbourhoods. One government party was infavour of volunteer police services (Sicherheitswacht), and the other wanted to establish neighbourhood watches corresponding to the US model. It ended up as “strong state” vs “strong citizen”- discussion. The opposition claimed that NW was viable, and then the government reproduced every clichés possible about civil engagement in security issues. There were claims about “Bayern-Stasi”, and “informership”/grasses, “…which has its predecessors among the Blockwart.” As such, the “Sicherheitswacht” chosen. Since then, NW emerges during election campaigns (see SZ 19.10.1996 on the land level) or every time a local council has decided to apply for having a Sicherheitswacht in town. Then there’s a call for applications, with information about which criteria have to be met and how good or bad this idea works in other towns of the area.

Media discourse about “Neighbourhood Watch” also emerges after specific events e.g. xenophobic hate crimes such as Solingen 1992), 9/11 and especially the terrorist attacks in London and Madrid (See SZ, 9.12.2005), but also after single acts of brutal violence among youths (Berlin, Alexanderplatz 2012), there are discussions about appropriate measures of prevention. In these discussions, the typical arguments of the “more-police-vs-more-civil-engagement” debate are repeated (often complemented by calls for more CCTV).

A second line of reports are those incited by specific crimes – such as burglary – that demand “on site-solutions”: A report from a NW member in UK shows, how police activities are insufficient and how citizen efforts are also important.[123] However the demand for neighbourhood watch to prevent burglary is not very successful, since initiatives like “Wachsame Nachbarn” coordinated by the police already fill that vacancy. Then there is a third line of discourse: Active, responsible citizens/neighbourhood are called for because of a perception of disorder or of anti-social behaviour. A report about US Neighbourhood Watch members[124] depicts an almost heroic citizen, who reclaims the streets of his hometown from drug dealers at night, together with his neighbours. Furthermore, the person reports of how positive his relationship with his neighbours has developed, since they found out that they had problems they shared and joined their efforts to face them. On a smaller scale, something similar can be observed in a town in Schwaben: here, an initiative among neighbours, involves them reporting about smashed bottles, condoms and syringes on playgrounds. The police perceived this problem to be outside their remit, and so the community acted instead. In the end, the initiative has not got the necessary permission and people are advised to cooperate more strongly with the police. Acting without the police is generally considered to be dangerous, it could even worsen the situation or is ineffective in an “absurd manner”.

The German press sometimes reports on NW activities from around the world to illustrate the dangers of vigilantism, and, by extension NW. For example, one paper reports “The

[123] Zeit, 23.7.1993: “We are all Deputies”
[124] Zeit, 3.11.1989

shock about 9/11 has led to a security mania even in private life. In the Wild West, people bought guns and they founded vigilante groups. Today they buy CCTV cameras and denunciate suspects within the scope of Neighbourhood watch."[125] (In Littleton for example, there's an increased number of Neighbourhood watch schemes after the Columbine High School massacre:

> "The massacre left a desire for revenge, a demand for a scapegoat, no matter how little it may be. This has also sharpened the focus on seemingly unusual behaviour within the local Neighbourhood watch scheme. And if there is nothing to report on, even the denunciation of kids behaviours is appreciated." [126]

Negative reports reached their climax in 2012, when a young man was shot by a Neighbourhood Watch member in Miami.[127] This confirmed nearly all prejudices against private or civil efforts in security issues.

In *Spain* communities tend to be polarised either in favour of or criticising NW, but there is no great engagement with NW itself. The emergence of patrols tends to take place after particular events covered in the media or in relation to a perceived local problem. Examples include insecurity, drug abuse, migration and the economic crisis, which are the major problems perceived by the Spanish population. The existence of citizen patrols for this report was only confirmed after an extensive media analysis.

Finally, NW is still very popular in the *UK* and public engagement with it is high. 3.8m households in England and Wales are members. Current numbers of schemes (late 2013) were: Scotland – 1,600; England and Wales – 12, 000, and Northern Ireland – 770, but the actual total number of schemes is thought to be much higher as many schemes do not register with the national co-ordinating bodies.

[125] SZ, 24.4.2008
[126] Zeit, 28.19.1999
[127] For example, SZ, 23.4.2012

All NW members are volunteers, they are unelected, groups tend to number around an average figure of 20, they are not normally subject to criminal records checks, they are not uniformed, they tend to be aged over 50. Groups are most commonly formed in more affluent areas, and less commonly found in poorer areas, which may have a higher density of social-rented housing and mix of ethnic communities. Members are not thought to have undertaken any acts of vigilantism, although the Neighbourhood and Home Watch Network (for England and Wales) issued a statement in 2011, around the time of major rioting in some of the UK's cities, warning neighbourhood watch groups not to engage in any acts of vigilantism. Instead they were urged to forge stronger links with the police. Neighbourhood watch schemes will commonly have a constitution, but they do lack democratic legitimacy in the strictest sense, as members are unelected. The media are generally disinterested in the activities of NW because they are not particularly controversial or sensational. In fact NW has been parodied in British popular culture –most notably in the film 'Hot Fuzz' (2007)[128] – where they were portrayed as having more surveillance powers than the police and as officious, interfering busybodies.

In summary, democratic intersection with citizen-citizen surveillance is very sparse indeed because in three out of four countries it is not recognised as a legitimate way to reach the societal goals of community safety and crime prevention. In Austria and Germany there is no tradition of forming NW as a response to such problems as there is a strong cultural preference for, and deference to authorities in these matters. NW has become a political football in these countries, with right wing politicians stirring up alarmism about right wing extremists and left wing politicians becoming concerned about vigilantism. In Spain it is completely unregulated and not a priority for law enforcement agencies. Public interest ebbs and flows and informal 'patrol' groups emerge in relation to particular threats, stoked by social media. The unique case is the UK, where surveillance and NW is more normal and less controversial than in the other countries. The UK has never experienced authoritarian or

[128] See, http://www.imdb.com/title/tt0425112/

fascist government in its recent history. Although NW has a registry it is not referred to in any policing related statutes, it is governed by charity law. Media interest is low although NW interacts with local police and government as part of broader community policing strategies.

IV. 5 Improving democratic resilience in the face of NW

In section IV.3 of this report we identified 5 harms across the case study countries which had emerged as a result of NW. These harms concerned the stigmatisation and restigmatisation of communities and places; physical harm; invasions of privacy; the normalisation of surveillance and questions over the privatisation of security. The harms occurred in different configurations in each country.

In *Austria*, where NW had emerged as a counter movement to public schemes, the main harm we observed were privacy issues arising over the creation of crime databases by the NW schemes. In *Germany* among very unfavourable opinions about NW, negative media coverage revealed that stigmatisation, especially on grounds of race, had been a problem in the past where right wing extremists had infiltrated the voluntary police. There was an incident of physical harm inflicted on an individual by one scheme via the use of pepper spray. This was a turning point for that particular NW scheme as its members were prevented from carrying any equipment or identifying themselves with a uniform. There is also a concern about the privatisation of security in Germany where the state is considered the only legitimate actor in this domain. Scare stories had been reported in the media about US NW schemes where citizens had taken matters into their own hands and created further harm. In *Spain*, after NW patrols emerge, police tend to react by deploying more officers to affected areas and there is subsequently greater communication between police and citizens but this is generally not sustained in the longer term. Restigmatisation of areas by one vigilante group has sometime prompted counter action by another. In the 1980s such vigilantism actually resulted in the physical harm of drug addicts on the Barcelona streets. Privacy is also seen as a risk by stakeholders given the more widespread use of social

media, and even unmanned aerial vehicles by ad hoc community safety groups. Finally in the *UK*, no specific harms were associated with NW, although privatisation of security was a clear concern in the climate of government funding cuts for public services such as policing.

To address democratic resilience in the face of harms created by NW, we should first note that NW is taboo in cultures which have experienced authoritarian or fascist i.e. profoundly un-democratic pasts. In each of those histories, local surveillance by community members towards their fellows has unduly negative connotations. It is a dangerous possibility as it has legitimised discrimination, oppression and a lack of accountability in the past. If community safety and caring community values are what is valued in those places then it seems NW is not the way forward. Despite the fact that ad hoc NW schemes emerge from frustrations with the police, the answer seems to be strengthen police funding and improve community relations with the police per se. So, strengthening democratic resilience in the face of harms created by NW in Austria, Germany and Spain around stigmatisation and violence will revolve either around improving intra-community relations in general, rather than mobilising the community to counter a particular threat; or around better community policing strategies i.e. by further democratising local police provision. Tackling the privacy problems arising from the ad hoc use of social media and the creation of databases by NW groups would also result if community groups were advised in the right way about this issue. In the UK, where there have been few problems, using NW as a vehicle to further democratise community policing would improve on the current situation.

To address democratic resilience in the face of NW is a two edged sword. First, resistance to NW initiatives in Austria, Germany and Spain seems to be borne out of the notion that the capacity to surveil for crime and safety purposes lies within the remit of government institutions. As such this denotes a form of resilience to attempts to enrol the citizenry in surveillance. There are two lines of reasoning here. In Austria and Germany this resilience is based on the belief that law enforcement institutions should be maintained and reinforced.

In Spain this resilience is based on a general cynicism about the efficiency and effectiveness of law enforcement institutions. Second, we have revealed that NW is taboo in cultures which have experienced authoritarian or fascist i.e. profoundly un-democratic pasts. In each of those histories, local surveillance by community members towards their fellows has unduly negative connotations. It is a dangerous possibility as it has legitimised discrimination, oppression and a lack of accountability in the past. If community safety and caring community values are what is valued in those places then it seems NW is not the way forward. Despite the fact that ad hoc NW schemes emerge from frustrations with the police, the answer seems to be to strengthen police funding and improve community relations with the police per se. So, strengthening democratic resilience in the face of harms created by NW in Austria, Germany and Spain around stigmatisation and violence will revolve either around improving intra-community relations in general, rather than mobilising the community to counter a particular threat; or around better community policing strategies i.e. by further democratising local police provision. Tackling the privacy problems arising from the ad hoc use of social media and the creation of databases by NW groups would also result if community groups were advised in the right way about this issue. In the UK, where there have been few problems, using NW as a vehicle to further democratise community policing would improve on the current situation.

CHAPTER FIVE

SYNTHESIS AND CONCLUSIONS

The final section of this report synthesises the case study findings around four key issues. First, patterns of democratic intersection with the three surveillance practices examined in the report are considered. Then, the macro variables which produce some of the key differences between the practices in each country are mapped. These variables are based on the factors identified in Work Package two. The harms produced by the practices are then presented and discussed. Finally, some suggestions for increasing resilience are made.

V.1 Patterns of democratic intersection with surveillance practices

Table V.1 illustrates the intersection of different democratic practices with the surveillance practices we have examined across the cases. Within the ANPR case we observed variable forms of governance, ranging from top down constitutional governance within Germany to minimal governance in the United Kingdom. Stakeholder participation was very limited apart from in Germany who had constitutional court rulings which limited the processing of data collected by ANPR cameras. There is also low public engagement with ANPR, partly because regulation has not yet caught up with practice and ANPR cameras are not required to be specially signed. It is difficult to know whether one is subject to ANPR or not. There has been some activist and campaign engagement, however, which has resulted in media coverage in all of the case settings.

Credit scoring had strong centralised governance in all cases, given that the financial services industry is regulated at a European as well as at National level. There was variable involvement of Data Protection Authorities (DPAs), however. In Norway the entire credit scoring system was premised on data protection regulations. In the UK credit scoring data are easily available without reference to the DPA. In other countries there was next to no

involvement of DPAs. Stakeholder participation is low, although financial services authorities and credit bureaux readily share information to enhance their risk assessment of customers. In Italy financial information is also shared with government for tax purposes. Finally, in Norway and the UK there is high public engagement with credit scoring but in Austria, Hungary, and Italy there is minimal engagement, with the exception of a few court cases.

Neighbourhood watch itself is a democratic idea, premised, as it is in the Anglo American model at least, on active citizenship around local crime and community safety. However it is also premised on local neighbourhood surveillance, which in post-authoritarian and post-fascist contexts is taboo. Hence, there is low governance, participation and engagement in the three post-authoritarian contexts – Austria, Germany and Spain – we examined

	Governance	**Participation**	**Engagement**
ANPR (Belgium, Germany, Slovakia, UK)	Variable: Strong top down framework in Germany, DPA involvement Emergent in Belgium, some DPA involvement Piecemeal in Slovakia, no DPA involvement Nothing in the UK outside of ACPO	Low except Germany, with court rulings mobilising information self-determination rights	Low with the exception of activists/campaign groups
Credit Scoring (Austria,Hungary Italy, Norway, UK)	Strong and centralised in all cases. Variable DPA intervention: High- Norway Low – the rest	Low, other than between watchers who share information.	High in Norway and the UK Low in Austria, Hungary and Italy
NW (Austria, Germany Spain, UK)	Low in all countries, no legal governance. Central registries of schemes in the nations of the UK	Low. Limited to directly interested parties and the media in Austria, Germany and Spain Government funding and Police involved in the UK	Low in Austria, Germany and Spain, sensationalised in the media Medium in the UK, parodied in popular culture

Table V.1: Patterns of democratic intersection across the cases

In the UK there is very little regulation, some wider stakeholder participation and quite widespread engagement. This is perhaps because widespread surveillance is more culturally acceptable although the tenor of neighbourhood watch is changing towards one of 'good neighbourliness and community values' from that of localised suspicion and spying.

Overall, patterns in governance and engagement are variable, the reasons for which will be explored in the forthcoming sections as they are associated with the peculiarities of the practices. However one identifiable pattern across the three practices of ANPR, Credit Scoring and Neighbourhood Watch is that peripheral stakeholders in all of the practices are not involved in how the watcher/watched nexus is shaped. This lends support to many previous observations that domains of surveillance tend to be inward looking with their preferred sets of institutions, practices and power relations (Surveillance Studies Network 2006; Latour 2005)[129]. The reasons for this are different however. ANPR, as a partially regulated law enforcement and security practice which is sometimes deputised out to the private sector. As a technology-enhanced security practice decisions about its specifications and deployment are taken far from the public domain. As we see in all of the countries, any questions about the location of cameras, assessments of their impact and any complaints about how they are used occur further down the line. As ANPR is so closely tied to the operation of the rule of criminal and road safety law (except for the Slovakian case) the parameters of its deployment are limited to law enforcement agencies and its suppliers. However the nature of the harms created by ANPR indicate that earlier discussions are a good idea.

Credit Scoring, by contrast, is a commercial practice and many of its internal parameters are the subject of commercial confidentiality. Financial services organizations have their own strategies in terms of the customers they target and how risks are managed in relation to those customers. Revealing those to external stakeholders would be regarded as commercially unwise. Credit bureaux, which trade on the analysis of consumer financial data

[129] Ibid n. 3; Latour, B (2005) Reassembling the Social. An Introduction to Actor-Network-Theory. Oxford: Oxford University Press

would have similar views. However, given the harms we have uncovered surrounding malpractice and the abuses of power surrounding credit scoring, financial services organizations would need to be given an opportunity to respond as well as clearer regulatory guidelines associated with credit scoring competence. Greater regulatory powers in terms of punishing financial institutions in the case of malpractice as well as customers who are pro-actively informed about their rights is needed. Finally, participation in neighbourhood watch is very low apart from in the UK because of the taboo associations NW has in post-authoritarian or post-fascist countries. In the next session discusses the parameters along which the cases varied and then proceed to discuss harms in more detail.

V.2 WP2 macro factors and within- and between-case differences

Chapter I of this report argued that factors identified in WP2 would produce variation in the configuration of surveillance practices in different national contexts. This section identifies these factors, which stem from the legal, political and social analysis offered in WP2. Each set of factors is presented in a diagram for ease of reference and then the diagram is described. ANPR, Credit Scoring and Neighbourhood Watch are discussed in turn.

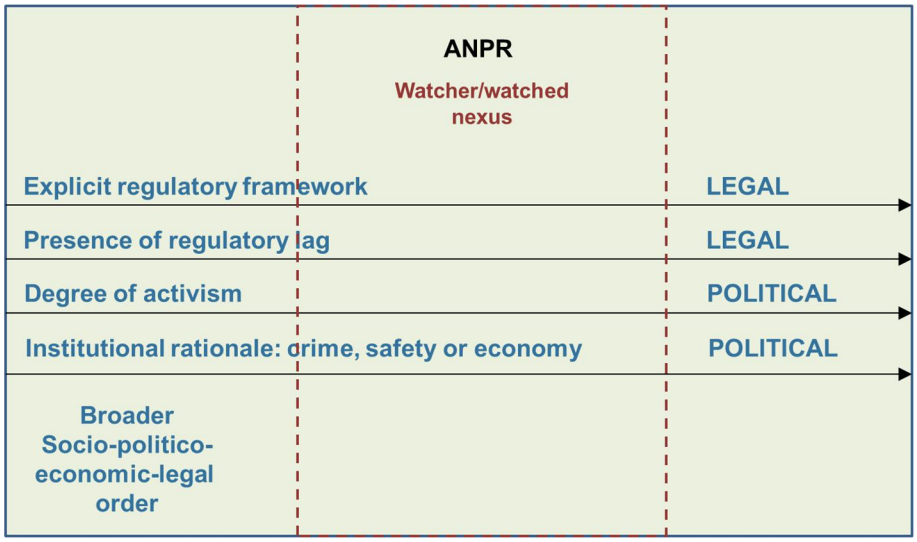


Figure V.1 ANPR Macro Factors

Figure V.1 outlines the factors which affect ANPR across the case countries of Belgium, Germany, Slovakia and the UK. Variation in the regulatory framework was identified,

discussed in section V.1. Regulatory lag, where regulation about surveillance lags behind what the technology can do was recorded in Belgium and Slovakia, but not in the UK or in Germany. Germany has robust regulation and the UK has not shown any intention of regulating ANPR more formally. Across the cases, activism has highlighted the problems which ANPR poses and has gained media attention for it. It was also observed that ANPR can be introduced under a variety of rationales which itself delineates the harms and consequences observed. The latter two factors are political in nature and the former are classified as legal in nature.

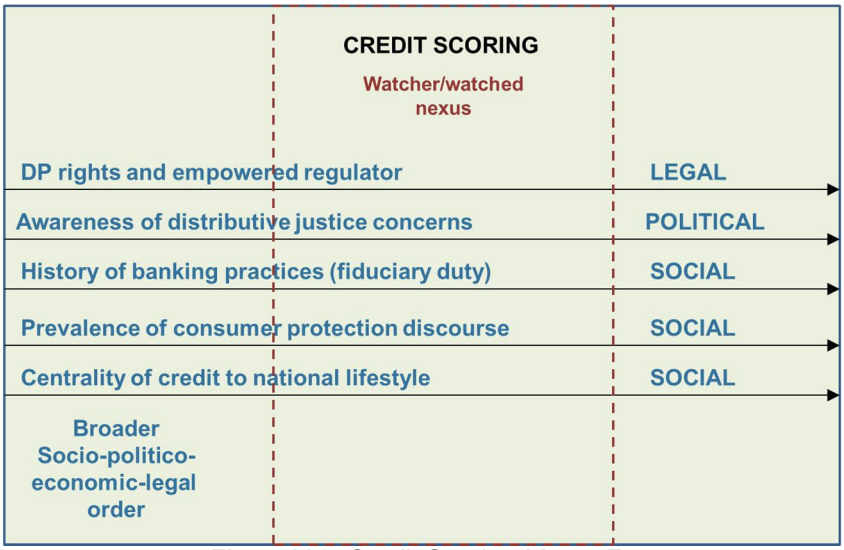


Figure V.2 Credit Scoring Macro Factors

Factors which seem to explain the shape of credit scoring across the case study countries of Austria, Hungary, Italy, Norway and the UK are legal, political and social in nature. The legal powers of respective Data Protection Authorities over credit scoring very greatly, with the Norwegian DPA having the greatest remit and Hungary, Italy and Austrian DPAs having barely any powers or interest in the practice. Similarly Norwegian authorities show good awareness of the distributive justice consequences of credit scoring, whereas other countries do not. It was quite clear that the history of banking practices and values, particularly concerning the fiduciary duty of client confidentiality, commercial secrecy as well as values of autonomy in financial institutions seemed to proscribe how much institutions felt they could be open about credit scoring. Consumer protection discourse was highly variable,

being more prominent in Norway and the UK, who were open about credit scoring, and non-existent in the other countries. The final, and very important factor is the role of credit in consumer lifestyles. In the countries which are more open, credit plays a central role, whereas it is less important in the other countries. The latter three factors are classified as social factors, the first as legal and the second as political.

Finally, the factors which affect the variation observed in the Neighbourhood Watch case are shown in figure V.3. They are political and social in character. The first relates to the issue we have already discussed concerning the political history of the respective country and the extent to which it accepts informally organized surveillance in a locale. The second relates to the extent to which police are the only body for which it is legitimate to tackle crime, disorder and community safety. In Germany and Austria the police are considered the only body for whom it is appropriate to deal with these matters. The community is not encouraged to do so. The qualitative history of police/community relations, however, can also create norms about what communities can expect from the police. Finally, frustrations with community policing led to the NW-like organizations to appear in all of the cases.

Figure V.3: Neighbourhood Watch Macro Factors

V.3 Patterns of harm

In Chapter 1 of this deliverable, the categories of harm identified Surveillance Studies' Network's 'A Report on the Surveillance Society' were used to scope what might occur in relation to the cases. To recap, matters for concern identified by SSN were as follows:

- *Social sorting*: a digital categorisation process affords which opportunities for some and disadvantages for others producing distributive justice concerns.
- *Unintentional control*: one person's management may be another person's social control. Surveillance signifies different things to different social groups, which may create perceptions of harm.
- *Information sharing*: the desire to get things done may result in data protection and privacy being overlooked.
- *Blurring of the public and private in surveillance systems*: The complexity of some surveillance systems which cross organizational boundaries can exacerbate problems of data protection as well as blur the locus of governance and regulation.

SSN then identify several harms which result from these characteristics of surveillance:

- *Anonymity and Privacy*: because of the ubiquity of surveillance systems and the presence of unique identifiers about our person, either via our phones, vehicles, ATM and credit cards or TCP/IP addresses, it is increasingly difficult to achieve anonymity. Thus, one of the first pillars of privacy, anonymity, is compromised by surveillance practices.
- *Choice and consent*: While the issue of consent arises straight away in relation to data processing surrounding information from various unique identifiers, there is little opportunity to opt out of surveillance.
- *Discrimination: speed, access and social inclusion*. As social sorting delimits choices and sets category boundaries which ascribe advantages and disadvantages to social

groups. The result of this social sorting process is enhanced access and convenience for some, and increased barriers for others.

- *Democracy, accountability and transparency*: Governance, participation and engagement can be compromised in a surveillance society and leave citizens feeling ill equipped to challenge or question surveillance practices

Each of the cases exhibited a different set of harms which maps on to the issues identified by SSN in a surprisingly accurate way. The ANPR case is presented first.

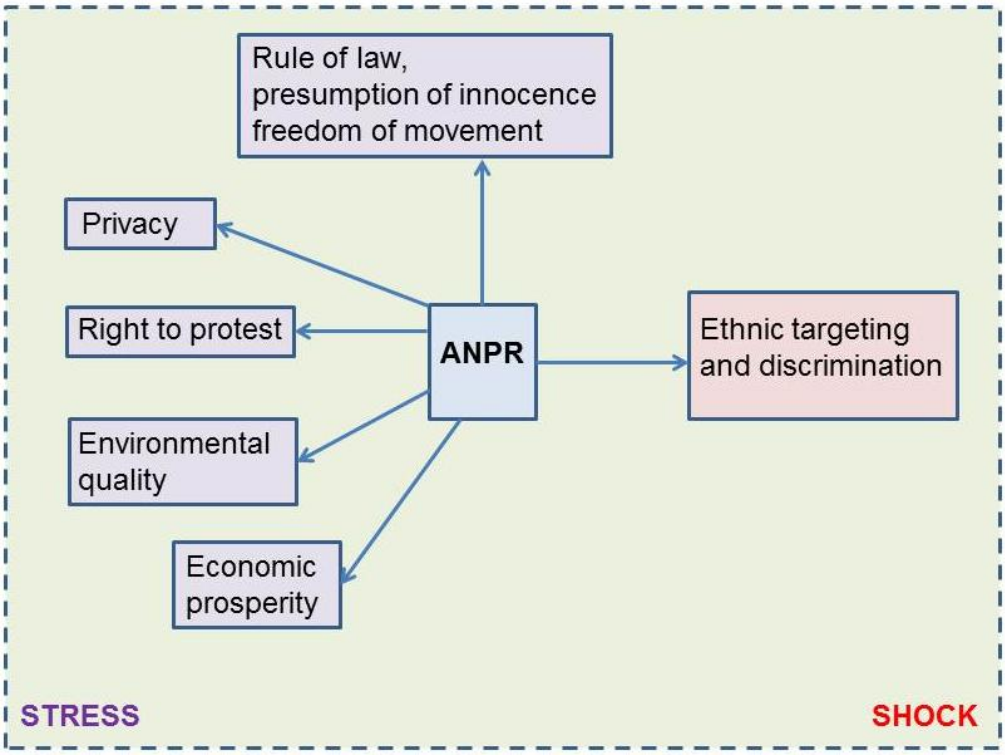


Figure V.4 ANPR Stresses and Shocks

ANPR resulted in some profound stresses and shocks. Three stresses and the one shock were already anticipated in a surveillance society by SSN. The case studies found evidence that use of ANPR had circumvented and breached the rule of law, compromised rights and had raised privacy issues. In the least regulated country, the UK, it had been found to affect detrimentally the right to protest and had deliberately been deployed in a racist way by police in Birmingham following Project Champion. However the situation in Slovakia extended the harms observed by a surveillance practice. In an effort to avoid the economic losses

imposed by road tolls, Slovakian truck drivers had taken to driving on smaller roads and affecting the quality of life for the villages which were located on those roads.

Stresses rather than shocks were uncovered in the credit scoring case studies. This case uncovers problems with the general characteristics of surveillance pointed out by SSN: that it is a management process which centralises power. The harms uncovered which related to administrative matters highlight how this form of surveillance is explicitly part of a management process and hence subject to administrative errors. However evidence was also uncovered of bank and legal staff abusing their position in relation to this sensitive financial data (Austria, Hungary). Similarly its location in the commercial sector meant that some unscrupulous organizations exploited it to facilitate the lending money to customers who could ill afford it and were financially illiterate (UK). Overall this points to a problem with transparency and with the operation of the rule of law in relation to credit scoring (Italy, Hungary, Austria). The distributive justice aspects of credit scoring and its ability to delimit economic prosperity were noted in the UK and Norwegian cases particularly.

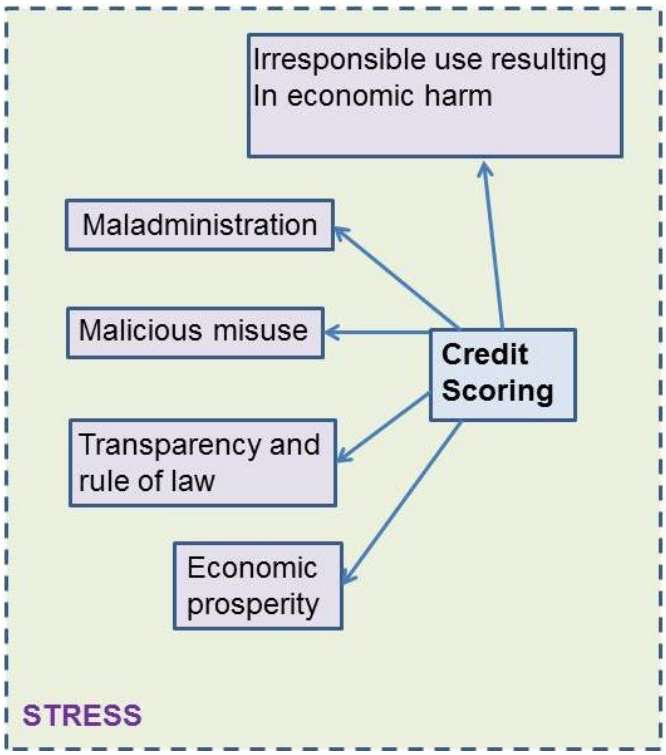


Figure V.5: Credit Scoring Stresses

Figure V.6 illustrates the stresses and shock which emerged in the Neighbourhood Watch case studies. Privacy was a relatively minor issue in these cases. The cultural and social significance of surveillance was far more powerful and generated strong sentiment towards it as a community safety idea (Austria, Germany, Spain). In these cases surveillance processes became controversial because as well as creating unhelpful links with the past, it was feared that they would present opportunities for extremists of all political colours. Indeed this was observed as a shock in the German and Spanish cases. The presence of NW-like organizations stigmatised particular spaces and focused on victimising those who were perceived as 'other' at that moment. It also challenged policing authorities who, at a community level, tread a fine line between too-little or too-much intervention, leading to a rise in feelings of security if crime appears to be increasing.

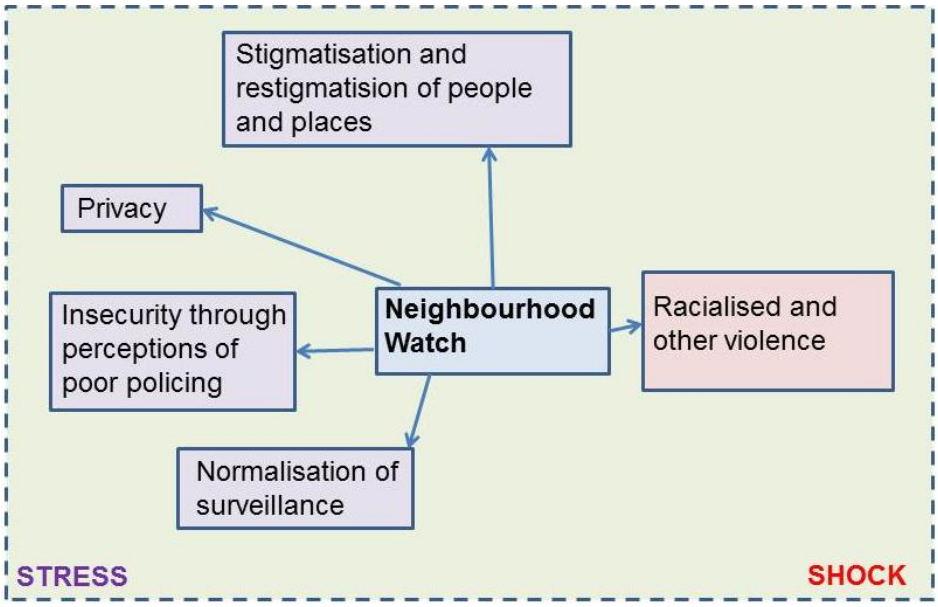


Figure V.6 Neighbourhood Watch Stresses and Shock

Summary

The stresses and shocks uncovered in these cases augment those identified by SSN. The findings underpin issues they associate with social sorting (Credit Scoring), unintentional control (Neighbourhood Watch), information sharing (ANPR, Credit Scoring), public/private blurring (ANPR, Credit Scoring) privacy (all cases), choice and consent (ANPR, Credit

Scoring) Discrimination (all cases) democracy, accountability and transparency (all cases). The issues of economic harm (ANPR, Credit Scoring) and environmental quality (ANPR) have augmented this list.

V.4 CONCLUSION: Surveillance, the limits of democracy and resilience

In Surveillance Studies, surveillance is referred to as having a number of characteristics, an origin and a set of consequences which are always emerging. Surveillance is a fundamental social process which is characteristic of all societies. Societies cannot function without lines of sight between individuals, groups, within families and organizations of different types. It helps to create hierarchy, internal order, it helps to distribute resources and create senses of right and wrong. This was the case in pre-industrial societies as it is now. However with the advent of the modern bureaucracy, urbanization and the informatisation of all manner of social processes, the remit of surveillance extends beyond interpersonal relations and uses extensive and intensive data collection analysis and applications to influence and control what people do and when. In the present day, surveillance is a process which involves the collection of and attention to personal information about a population in order to influence and manage what goes on within that population. It is a process which is systematic, it is always deployed with a particular purpose in mind, there is nearly always a strategic intent behind its deployment, and it frames the world in rational, positivist terms (Lyon 2001)[130]. It is a set of practices which is connected to all kinds of governance, involves the coagulation of power in particular actors and is nearly always deployed against a risk or a threat. Without risk, there is no surveillance. Indeed each of the case studies highlighted how its respective surveillance practice was deployed to counteract a particular harm, in the interests of the state (ANPR), a private sector organization (Credit Scoring) or the community at large (Neighbourhood Watch).

[130] Lyon, D (2001) Surveillance Society: Monitoring Everyday Life London: Open University Press

The surveillance society' is referred to in similar terms. It is a society, one of whose dominating organizing principles is that of the collection, recording, storage, analysis and application of information on individuals within that society, as they go about their daily lives. As people's daily lives have many different aspects ie work, consumption, travel, citizenship etc these form different 'domains of surveillance'. Within these domains of surveillance there are different kinds of actor – institutions, business organizations, governments, regulators, individuals and groups of individuals within a population - who are subject to different kinds of data collection, classification and influence. Our case studies have shown that the three surveillance practices are heavily embedded in historical practices and institutional norms, social beliefs and political systems.

It follows that surveillance societies are not singularities or monoliths; second that the boundaries between domains and their components are porous and finally, that surveillance is a process which has consequences. As Lyon, Haggerty and Ball (2012) [131]argue:

'it has produced downstream social changes in the dynamics of power, identity, institutional practice and interpersonal relations on a scale comparable to the changes brought about by industrialisation, globalisation or the historical rise of urbanization' Lyon, Haggerty and Ball 2012

The case studies presented in this report explore and exemplify some of the current issues in surveillance. In the case studies of ANPR and Credit Scoring we saw that boundaries were blurring between institutions. ANPR systems were commissioned and run by private companies to the end of law enforcement and financial institutions shared data with each other to enhance their risk assessment of customers. Surveillance is become more visible and invisible at the same time. Many European citizens are familiar with surveillance cameras, but it is increasingly difficult to know what kind of camera is operating – whether it is digital or not - and what is done with the information that is collected. In a perverse way,

[131] Lyon, D, Haggerty, K and Ball, K (2012) Introduction: Understanding Surveillance In Ball, K, Haggerty, K and Lyon, D (2012) The Routledge Handbook of Surveillance Studies London: Routledge

it's even possible to argue that surveillance has become democratized, in that hardly anyone is missed out nowadays, but that inclusivity is not matched with empowerment over one's involvement via an effective rights framework. As such, we can surmise that the privacy infrastructure may have fallen short so there is a recurrent question about how the vulnerable, and the human rights of everyone, are protected.

As surveillance, via the means of databases, huge information infrastructures, and the application of data analytics in all manner of domains, becomes more heavily intertwined with the activities of business and the private sector, it becomes ever more intransparent and, in Huysmans' (2014)[132] terms, begins to enact the limits of democracy. It becomes most relevant, therefore to question how democracy can become more resilient to the harms surveillance poses.At the beginning of this report we distilled four notions of resilience in relation to surveillance. These four notions were derived from the position that surveillance is deployed to counteract harm, threat and risk, but that it simultaneously has harmful, risky or threatening consequences.

- Surveillance as a strategy to counter risk produces two types of resilience:
    1. *Resilience to and reduction of harm through increased safety and security:* When surveillance counters risk or threat in an effective way, increased safety, security and economic prosperity are experienced. The means of surveillance renders society more resilient to security, safety and economic threats.

    2. *Resilience to surveillance by understanding its benefits:* If surveillance is commonly understood as an effective means of counteracting threat, then it becomes normalised and accepted more readily. Its harms are perhaps more readily accepted and are seen as being outweighed by its benefits.

[132] Ibid. n 9

- Surveillance as producing risks, threats and harms:

3. *Resilience through the chilling effect:* When surveillance produces harm, chilling effects have also been observed as rights are denied and civic engagement declines. The chilling effect represents a homogenisation and/or stagnation of social, economic and democratic processes, as society puts its 'head in the sand', preferring to ignore what is going on. It is a very unproductive type of resilience to surveillance.

4. *Resilience through increased awareness of surveillance and privacy and the development of critique:* If different sections of society engage with the harms produced by surveillance, resilience to its harms emerges in critical discourse against such surveillance practices and increased resistance to them. This also includes the discourse on consumer protection, data protection and constitutional law.

These four notions of resilience were constructed on the assumption that core stakeholders – watcher and watched (in particular) – would have prior knowledge that they were engaged in a surveillant relationship and knew the terms of that engagement. When the cases were assessed, however, this position was not a consistent one. In the ANPR case, with the exception of Germany, very low engagement of the watched was evident because of a lack of consistent regulation and signage, low levels of general media coverage and low engagement of data protection regulators with the practice. In the credit scoring case, with the exception of Norway and the UK, there was minimal public engagement and low awareness of the practice. For the watchers - those organizations in whose favour surveillance was deployed - surveillance produced several benefits. These benefits included better risk management and traffic law enforcement which has almost made the watchers immune to recognising that any harm may arise. Nevertheless, activist groups and the media have been working hard to highlight the harms associated with specific instances of ANPR (UK, Slovakia, Belgium), and Credit Scoring (UK, Norway) but changes in governance are

also needed to limit the effect of those harms. Neighbourhood Watch is a special case in that, with the exception of the UK, it has developed outside the remit of law enforcement institutions. However the experience of NW in the case study countries is simultaneously an example of community resilience and community breakdown. In an attempt to create community safety its harms stem from frustration with 'the other' and insecurities in relation to community policing. The British example, with minimal regulation and a caring focus, show how NW can succeed without the deep levels of mistrust and unpleasant associations which stem from authoritarian pasts.

Given these low levels of engagement, it is difficult to suggest that effective democratic mechanisms are in place, at European and at country level, which mitigate the harmful effects of surveillance in a resilient way. This is observed in places, but it is not the norm. Indeed the cases are dispersed around Murakami Wood's (2012)[133] framework which shows, again how democracy's limits are becoming enacted by surveillance. Murakami Wood (2012) has identified a number of ways in which state governance intersects with information flows to produce different types of surveillance society.

- *Adiloptic Democracy* (literally, blind seeing) features a strong rights framework in very low information flow. The low information flows in Neighbourhood Watch coupled by the complete freedom of choice for citizens to join or not, places it in this category. **Neighbourhood Watch: Austria, Germany, Spain, UK**
- *Synoptic Democracy* ('all together seeing') couples medium levels of information flow with a strong rights framework. The strongly constitutional response of Germany to ANPR, which limited information use gathered by the technique, places it in this category. **ANPR Germany**
- *Perioptic Democracy* ('all around seeing') couples high levels of information flow with a strong rights framework and creates a reciprocal surveillance society. Norway's

[133] Ibid. n. 4

building of a credit scoring system on data protection principles and the open-ness of this system places it in this category. **Norway credit scoring**

A further category of state he refers to is the Polyarchy, where power is dispersed among several large actors, such as the state and its various organs as well as the private sector.

- *Adiloptic Polyarchies* emerge. These states are limited democratic states that do not depend on information to function. The state becomes very opaque in an adiloptic polyarchy. No case studies were placed in this category.
- *Oligoptic Polyarchies*. (a few can see) produces a regulated surveillance society. In these kinds of society the state processes, uses and disseminates information but has a lot of choice in terms of how it does so. The use of ANPR and emergent regulatory frameworks in Belgium and Slovakia place it in this category. The semi-openness of credit scoring in the UK is also relevant. This openness is based on strong industry regulation rather than on data protection rights. **ANPR Belgium, Slovakia; UK Credit Scoring**
- *Panoptic Polyarchy* They have some democratic features but citizens are quite limited in their ability to access them. The centralisation of power in the UK ANPR case and in the credit scoring cases of Austria, Hungary and Italy place them in this category. **ANPR UK; Austria, Hungary and Italy credit scoring;**

The central finding of this report is that in order to increase resilience to the harms of surveillance across each case study, increased engagement with the nature and impact of those harms is needed on the part of both watchers and watched. Engagement may be achieved through enhanced media coverage, more robust freedom of information and subject access procedures, better public (ANPR) and customer (Credit scoring) information and subsequently regulatory powers and scrutiny of the institutions concerned can be increased.

To summarise our findings, box V.1 explains the WPs recommendations in relation to each surveillance practice. In relation to ANPR, in respect of very significant harms associated with privacy, freedom of movement, the rule of law, the right to protest as well as economic and environmental harms we observed different levels of governance which lagged behind technological capabilities. The first priority would be to harmonise governance with a European level directive. The gold standard developed in Germany, based on constitutional scrutiny and limitation of ANPR data collection would be a good starting point. Mandatory signage, enhanced DPA powers and the use of Privacy by Design in tendering processes for ANPR systems would perhaps feature in this directive. The provision of figures proclaiming the effectiveness of ANPR systems in detecting crime should also be made available by law enforcement agencies.

ANPR
- Harmonise legislation at European Level to German 'Gold Standard'
- Increased public awareness through signage
- Police forces to provide public information on the effectiveness of systems
- Strengthen DPA powers in respect of information gathered by ANPR
- Active tendering to include stipulations for privacy by design

Credit Scoring
- DPAs foreground procedural justice implications as per Norwegian 'Gold Standard'
- Europe-wide regulation of banks to increase accountability to customers in respect of credit scoring data
- Where consumer credit is in demand, officially inform consumers of their rights
- More vociferous media coverage of controversies resulting from Credit Scoring, as per the UK

Neighbourhood Watch
- Resistance to NW represents resilience to surveillance in post authoritarian contexts
- Strength police-community ties
- More police funding in order to strengthen those ties
- Improve intra-community relations

Box V.1 Increasing resilience

The first issue with Credit scoring is the public's awareness of and access to their own credit scoring data. While this is widely available in the UK and Norway, this is not the case in Austria, Italy and Hungary. Increasing transparency and accountability of financial institutions in relation to credit scoring data again could be instantiated at European level. Other countries could learn from the Norwegian model, which places DPA at the heart of

credit scoring and invests genuine powers in the courts to hear citizens' complaints about credit scoring practices. Following the credit crunch, demand for credit is now increasing across Europe and institutions should take this opportunity to inform consumers of their rights. Controversies associated with credit scoring appear in all of the case study countries, but in some cases the media have been slow to react, resulting in ill informed consumers and unaccountable, intransparent banks.

Finally the community reaction Neighbourhood Watch in Austria, Germany and Spain represents how those societies have become resilient to the surveillance they suffered at the hands of authoritarian and fascist governments. Improved relations within communities as well as between communities and police would further strengthen this resilience. Frustrations with a low police presence as a result of funding cuts (among other things) point to how this surveillance practice is intertwined with public resourcing issues. Whilst it is inevitably difficult to prioritise resource deployment in the current public financial climate, it is always important for police to be connected with the communities that they serve.

Overall the intersection between surveillance and democracy across the three case studies we have examined is varied. Patterns have emerged which are associated with historical, legal, political, social and institutional factors. At the dawn of the age of Big Data and as social life becomes constituted and reconstituted by layer upon layer of information infrastructures, the local and everyday contexts of our lives become readable and transparent to power. To a greater degree than ever before, surveillance processes intersect with and constitute the way in which we get things done. As consumption, communication, security and even democracy is done in this way – we need to question how transparency and accountability re-organize themselves as the traditional and institutional ways in which democratic power becomes enacted become less relevant. Perhaps a politics outside the conventional venues of power – one which focuses on the everyday, emphasises engagement, active citizenship and a reflection on the smaller things in life - which will enable alternatives to emerge.

References

ACPO Strategic Outline Business Case - ACPO TAM Business Area, available at: https://www.whatdotheyknow.com/request/36626/response/117902/attach/3/Disclosed%20information%20West%20Mids%20Business%20Case.pdf Accessed 27th May 2014

ACPO - Association of Chief Police Officers – (2005) ANPR Strategy for the Police Service 2005-8: Denying Criminals the Use of the Road, London ACPO

Ball, K and Murakami Wood, D (2006) Summary Report: A Report on the Surveillance Society. Wilmslow: Information Commissioners' office http://www.surveillance-studies.net/?page_id=4 accessed 27th May 2014

Banca d'Italia, *Centrale dei Rischi-Foglio informativo*, in Circolare della Banca d'Italia n.139/91, "Centrale dei rischi. Istruzione per gli intermediari partecipanti", http://www.bancaditalia.it/serv_pubblico/elenco-dei-servizi/info_archivi_CR/links/per-approfondire/foglio-informativo-CR.pdf Accessed 27th May 2014

Bennett, Trevor (1992) Themes and variations in neighbourhood watch, *Crime, Policing And Place: Essays In Environmental Criminology*, London: Routledge. pp.172-186.

Birmingham City Council (BCC) (2010*) Project Champion: Scrutiny Review into ANPR and CCTV Cameras*, Birmingham City Council, 02 November 2010, page 7.

Bonfondi M., Lotti L., (2006) *Innovation in the Retail Banking Industry: the Diffusion of Credit Scoring,* https://mail.sssup.it/~lotti/Bofondi_Lotti.pdf

Bolton, Sharon, *Crime prevention in the community: The case of Neighbourhood Watch*, Taylor & Francis, 2006, p.40.

Butcher, L (2009) 'Roads: Speed Cameras', *House of Commons Briefing Paper*, Standard Note: London, House of Commons Library, p. 5.

DiePresse.com (09.10.2013): Gerichtsvollzieher verkauften Justizdaten: "Na und ...?", http://diepresse.com/home/panorama/oesterreich/1462796/Interne-Justizdaten-verkauft_Na-und- accessed 10 Nov. 2013.

Donnelly, D (2008) Community Wardens in Scotland: Practitioners' Views, *The Howard Journal of Criminal Justice*, Wiley Online Library, 47, 4, pp.371-382.

Freeman, R. E. (1983). Strategic management: A stakeholder approach. *Advances in strategic management*, *1*(1), 31-60.

Fyfe, Nicholas R., (2013) Policing Crime and Disorder, in Donnelly, D and Scott, K (eds.) *Policing Scotland* Collumpton: Wilan. p.190.

Gandy, O. H. (2012). *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Ashgate Publishing, Ltd.

Goold, B., Loader, I., & Thumala, A. (2010). Consuming security? Tools for a sociology of security consumption. *Theoretical Criminology*, *14*(1), 3-30.

Greco A. M.,(2013) I giudici arrestano le tasse «Il redditometro è nullo», in *Il Giornale*, 27 September, p. 10

Gyenis, A (2007) “Az a fekete folt” [That black spot] *HVG* 2007/14, 07 April, pp. 107-108.

Haggerty, K. D., & Samatas, M. (Eds.). (2010). *Surveillance and Democracy*. London: Routledge.

Hayden, Evelyn (2003): *Are Credit Scoring Models Sensitive With Respect to Default Definitions? Evidence* from the Austrian Market, University of Vienna, Department of Business Administration Chair of Banking and Finance, Vienna.

Huysmans, J (2014) Security Unbound: Enacting Democratic Limits London: Routledge

Johnston, L., & Shearing, C. (2003). Governing security. *Explorations in Policing and Justice, London*.

Kenzel, Brigitte(2013) *Die automatische Kennzeichenfahndung. Eine neue Überwachungsmaßnahme an der Schnittstelle zwischen präventivem und repressivem Einsatz*, Verlag Dr. Kovaĉ, Hamburg

Krenn, Michael; Zeger, Hans G. (2009): *Datenschutzbestimmungen zur "Auskunft über die Kreditwürdigkeit"*, in: Bauer, Lukas; Reimer, Sebastian (Hg.) Handbuch Datenschutzrecht, Wien, facultas.wuv, S. 533-549.

Knyrim, Rainer (2008): *Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?;* in: ecolex Zeitschrift für Wirtschaftsrecht, S. 1060-1062.

Latour, B (2005) Reassembling the Social. An Introduction to Actor-Network-Theory. Oxford: Oxford University Press

Laycock, Gloria and Nick Tilley (1995) Policing and Neighbourhood Watch: Strategic Issues, *Home Office Police Research Group*, p.12.

Lyon, D. (Ed.). (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Routledge.

Lyon, D (2001) *Surveillance Society: Monitoring Everyday Life*. London: Open University Press

McConville, Mike, and Dan Shepherd (2013), *Watching Police, Watching Communities* London: Routledge

Murakami Wood, D (2012) Integrating Surveillance into Theories of the State: Towards a Model of Surveillance Societies. *Paper presented at the 5th Biannual Surveillance and Society Conference,* University of Sheffield 2 – 3 April 2012.

Murakami Wood, D et al (2006) A Report on the Surveillance Society Wilmslow: Information Commissioners Office. http://www.surveillance-studies.net/?page_id=4 accessed 27th May 2014

Nicholas, Siân, John Flatley (eds.) et al, (2008) Circumstances of Crime, Neighbourhood Watch Membership and Perceptions of Policing: Supplementary Volume 3 to Crime in England and Wales 2006/07: Findings from the 2006/07 British Crime Survey, Home Office

Norris, C and Armstrong, G (1999) The Maximum Surveillance Society London: Berg

Orsini C., *Da Basilea 1 a Basilea 3*, Arcadia Consulting Srl, Bologna, 2010, www.arcadiafinance.eu

PA Consulting (2004) *Engaging criminality – denying criminals the use of the road*, PA Consulting Group, London.

Emilia Papp, E (2007) "Eros lista" [Hot list], *HVG* 2006/05, 04 February, pp. 92-93.

Platt, John (1973) Social traps, *American Psychological Association*, 28, 8, p.641.

Plus Sedem Dní, Ďalší škandál (Another Scandal), 26/10/2010, available at: http://www.pluska.sk/plus7dni/vsimli-sme-si/dalsi-skandal.html, accessed 3rd November 2013

Schmiechen-Ackermann, Detlef (2000)„DER „BLOCKWART" -Die unteren Parteifunktionäre im nationalsozialistischen Terror- und Überwachungsapparat", in: *Vierteljahrshefte für Zeitgeschichte*, Vol 48 (4), p 575-602.

Sewell, G., & Barker, J. R. (2006). Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review*, *31*(4), 934-961.

Slovak Spectator, 21/10/2013, Changes To Electronic Toll System, available at: http://spectator.sme.sk/articles/view/51739/23/changes_to_electronic_toll_collection.html, accessed 16th December 2013

SME, Podpílili mýtnu bránu, zasahovala do cesty (Someone destroyed TollGate), 28/01/2010, available at: http://auto.sme.sk/c/5213337/podpilili-mytnu-branu-zasahovala-do-cesty.html, accessed 8th September 2013

SME, Rušičky z mýtnych ciest nezmizli (Jammers Still on Toll Roads), 30/05/2010, available at: http://s.sme.sk/r-rss/5399308/ekonomika.sme.sk/rusicky-z-mytnych-ciest-nezmizli.html, accessed 09 October 2013

SME, Polícia bude jazdiť na inteligentných autách (Police will drive intelligent cars), 20/09/2013, available at: http://auto.sme.sk/c/6941905/policajti-budu-jazdit-na-inteligentnych-autach.html, accessed 09th October 2013

SME, Kamionisti šetria na mýte a ničia domy i život v obciach (Trcks save on toll and destroy properties and life in villages), 24/08/2012, available: http://www.sme.sk/c/6509458/kamionisti-setria-na-myte-a-nicia-domy-i-zivot-v-obciach.html, accessed 09th October 2013

SME, Mýto vraj kamióny obchádzajú rušičkami, (Toll Is Allegedly Avoided by the Use of Jammers) , 26/03/2010, http://ekonomika.sme.sk/clanok.asp?cl=5302262, accessed 09th December 2013

Strobl, Gerhard; Hahn, Friedrich (2010): *Lehrgang für Finanzmarktaufseherinnen und -aufseher, Modul 1.07, Einführung Kreditgeschäft.* Aufsichtsakademie der Finanzmarktaufsichtsbehörde und Österreichischen Nationalbank, Skriptum, September/Oktober 2010.

Topping, John (2012) Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake http://eprints.ulster.ac.uk/22741/ Accessed 27th May 2014.

Titus, R. M. (1984). Residential burglary and the community response. In *Coping with Burglary*. Springer Netherlands. pp. 97-130

Thonabauer, Günther; Nösslinger, Barbara; Datschetzky, Doris; Kuo, Yi-Der; Tscherteu, Alexander; Hudetz, Thomas; Hauser-Rethaller, Ursula; Buchegger, Peter (2004): *Guidelines on Credit Risk Management – Rating Models and Validation.* Published by: Oesterreichische Nationalbank (OeNB), Financial Market Authority (FMA), Vienna.

Thornton, S. (2010) Project Champion Review: An independent review of the commissioning, direction, control and oversight of Project Champion; including the information given to, and the involvement of, the community in this project from the initiation of the scheme up to 4 July 2010; Thames Valley Police.

Westin, A. F., & Baker, M. A. (1974). Databanks in a Free Society: Computers. *Record-Keeping and Privacy Quadrangle*.

Weyrather, Irmgarth (1982) Die braune Fassade, Über d. Zusammenleben von Nazis, Kommunisten, Juden, Sozialdemokraten, Bürgern u. Arb. im *Berliner Mietshaus, Literatur und Erfahrung* 3 (10). p 44.

APPENDIX I: DATA SOURCES

Source	***Belgium***	***Germany***	***Slovakia***	***United Kingdom***
Activist websites				X
Data protection authority reports	X	X		
Email exchanges			X	
Freedom of Information requests				X
Interviews	X	X		
Legal literature	X	X	X	X
Newspaper articles		X	X	X
Online resources and social media	X	X	X	X
Parliamentary reports	X	X	X	
Police authority reports				X
Scholarly articles		X		X

Table A1: Automatic Number Plate Recognition case study data sources

Source	***Austria***	***Italy***	***Hungary***	***Norway***	***UK***
Interviews	X	X		X	X
Legal literature		X	X	X	
Newspaper articles	X	X	X	X	X
Online resources and social media		X	X	X	X
Scholarly articles	X	X			X
Subject access requests	X				

Table A2: Credit Scoring Data Sources

Source	***Austria***	***Germany***	***Spain***	***UK***
Email correspondence			X	
Media articles		X	X	
Meeting observation	X			X
Key informant interviews	X	X	X	X
Scheme documentation	X	X		
Scholarly articles				X
Social media			X	

Table A3: Neighbourhood Watch Data Sources

APPENDIX II: ORIGINAL CASE STUDY REPORTS

A. Automatic Number Plate Recognition:

B. Credit Scoring

C. Neighbourhood Watch

AUTOMATIC NUMBER PLATE RECOGNITION

(ANPR)

IRISS WP3 – Case studies – ANPR in Belgium

VUB - Final – Revised – January 2013

Antonella Galetta*

Introduction

It is widely recognised that ANPR (Automatic Number Plate Recognition) systems have a significant potential and remarkable comparative advantages with respect to other surveillance technologies.[134] Like other surveillance tools, ANPR cameras are deployed for security and law enforcement purposes and are usually considered as vehicle and traffic monitoring tools only. However, ANPR technologies can be used to reach many other aims which do not necessarily respond to crime-detection purposes. ANPR is particularly appreciated as system for controlling crimes and monitoring criminal activities, such as auto thefts and robberies. Nonetheless, these surveillance technologies can also help prevent crimes, as well as detect administrative offences linked to vehicle matriculation and circulation.

The use of ANPR technologies in Belgium is quite recent if compared to other countries across Europe, such as the United Kingdom. Although one could say that ANPR is still in an experimental phase in Belgium, it is noteworthy that its use is expanding. In fact, public governments and administrations are increasingly confident in and reliant on the use of ANPR systems and applications. Given their promising potential, it is foreseeable that the use of these tools will grow and that these technologies will be further improved in the future.

* The author thanks Tom de Schepper (Association of Flemish Cities and Municipalities, VVSG) and Caroline de Geest (Liga voor Mensenrechten) for their feedback, input and comments on this paper.

[134] See Parsons, Christopher, Joseph Savirimuthu, Rob Wipond and Kevin McArthur, "ANPR: code and rhethorics of compliance", *European Journal of Law and Technology*, Vol. 3, No. 3, 2012. Haines, Alina & Helen Wells, "Persecution or protection? Understanding the differential public response to two road-based surveillance systems", *Criminology and Criminal Justice*, Sage, Vol. 12, No. 3, pp. 257-273.

Little research has been conducted on ANPR systems in Belgium, on their benefits and risks and on the privacy impact related to their use. All this makes ANPR systems in Belgium a very interesting case study. After having looked at the history of ANPR in Belgium (Section 1), this paper will identify the main stakeholders and interests involved in the deployment of ANPR systems in Belgium (Section 2). This analysis will highlight emerging issues and controversies in the use of ANPR devices (Section 3). Special attention will be devoted to the regulation of ANPR in Belgium (Section 4), as well as to the media and public opinion (Section 5). The points of view of the watcher and the watched will be illustrated. From this latter perspective we will consider accountability strategies (Section 6) which may also consist in the exercise of access requests (Section 7). Lastly, we will focus on resilience in the use of ANPR in Belgium (Section 8) and summarise our findings in the conclusions.

1. The history of ANPR systems in Belgium

If one looks back at historical developments of ANPR in Belgium, one can easily recognise that the use of such technologies is the outcome of recent technological developments, advances and political choices. Generally speaking, ANPR represents a rising technology in Belgium, but there are no detailed studies on the subject and it is sometimes difficult to rely on accurate analytical data. Although a first nation-wide qualitative research about the installation of cameras in public places in 7 Belgian cities and municipalities was launched by the Belgian Ministry of Internal Affairs in 2012 (and released in 2013), it did not make any distinction as regards the type of cameras and the aims they were placed for.[135] Moreover, if one looks at the national level per se, there is not a clear-cut trend in the resort to ANPR, although recent developments indicate that more policy congruence on the national and regional level is emerging. Rather, one can find an array of different experiences and practices which have flourished at local level. In spite of this, it is possible to identify two key

[135] Mortelé, Jill, Hans Vermeersch, Evelien De Pauw, Wim Hardyns, Famke Deprins, “Cameratoezicht in de openbare ruimte. Ook wie weg is, is gezien?”, Maklu 2013, Reeks Politiestudies, nr. 6.

moments in the history of ANPR in Belgium. The first dates back to 2005 when the Local Police Force of *Politiezone Westkust* first introduced fixed ANPR cameras on public roads.[136] The second brings us back to 2012, when concrete initiatives were taken at national level to implement ANPR systems (see Section 2).

A system of number plate recognition was introduced in Brussels in 2008 through the installation of 172 cameras in the 24 tunnels of the city inner orbital road.[137] A wide network of fixed ANPR cameras was installed in the police district of Turnhout in 2010 mainly to detect traffic-related offenses (e.g. speed registration).[138] The city of Malines implemented an ANPR system in 2011 with over 20 cameras monitoring cars entering and leaving the city mainly for crime prevention and detection aims.[139] Apart from the use of ANPR systems on highways and roads, police forces are starting to test mobile ANPR technologies. Although there are no accurate data about the number of police vehicles equipped with mobile ANPR, the use of such devices is still very low. It is reported that at present the number of police vehicles endowed with an ANPR system (ANPR vehicles) is of 6 in Belgium in total (3 in the Flemish region; 2 in the Walloon region; 1 in Brussels). [140] So far ANPR have been deployed in Belgium both in larger-sized and small-sized municipalities. Moreover, it is remarkable that these systems result from a process of securitisation in which CCTV cameras gave way to

[136] Indeed, the *Politiezone Westkust* is the first police force in Belgium to have introduced public ANPR, as the police itself proudly reported in December 2013. See Politiezone Westkust, "Persmap Politiezone Westkust", 13 December 2013 http://www.lokalepolitie.be/sites/5461/images/teksten/persbabbel%2013%20december%202013.pdf (last accessed 23 December 2013).
[137] Survision, *Press Releases*, June 2008, Brussels, http://www.survision.fr/press/PR_2008_06_25.php (last accessed 8 October 2013).
[138] Belgacom, ICT News, *La Police vous voit*, *Les lecteurs de plaques minéralogiques améliorent la sécurité*, 24 September 2010, http://www.ictnews.be/fr/2010/09/24/the-police-are-watching/ (last accessed 8 October 2013). The police district of Turnhout includes seven municipalities, namely: Baarle-Hertog, Beerse, Kasterlee, Lille, Oud-Turnhout, Turnhout and Vosselaar.
[139] Blue Vision Telecom, *ANPR Project Mechelen*, 2011, http://www.bluevisiontelecom.be/news/anpr-project-mechelen (last accessed 8 October 2013).
[140] Rauwers, *Reportage RTL-TVI*, *ANPR Voiture Scanner à Liège*, 16 January 2012, http://www.rauwers.be/cms/index.php/fr/component/content/article/1-latest-news/150-anpr-reportage-rtl-tvi (last accessed 8 October 2013).

smart cameras.[141] Indeed, ANPR itself can be considered as sub-category of smart cameras and hence represents a sort of evolution of today's surveillance and securitisation processes.

ANPR technologies can have multiple applications and reach several purposes.[142] They are mainly used for detection of traffic offences in Belgium but they are also increasingly used as tools to combat crime. Considered as effective devices to ensure road safety, ANPR cameras scan number plates which are checked mainly against two different databases.[143] National vehicles are compared against the vehicle's directory for the identification of Belgian car number plates (within the Federal General Directorate for Mobility and Road Safety), whereas the Schengen Information System (SIS) is applied against European vehicles. The use of ANPR systems, in combination with the use of databases, let police forces know in a few seconds whether a certain vehicle is (im)matriculated, whether it has been subject to the technical control (and whether it has succeeded it) and whether its insurance is in force. Accordingly, police forces and the public administration as such use ANPR to claim fines and impose administrative sanctions. Secondly, ANPR cameras are used for vehicle speed detection. Information about the speed of a vehicle can be obtained either installing smart cameras which get such a measure by default (speed check cameras) or calculating the time the driver took to cover the distance between two ANPR cameras. Remarkably, Belgian regional and local governments are increasingly replacing analog cameras with digital and smarter devices, such as ANPR. Thirdly, ANPR can also detect administrative offences that refer to driving bans and traffic limitations. This is the case for

[141] Smart cameras are in operation on a permanent basis in e.g. Westkust, Malines and Turnhout. The municipality of Dendermonde uses smart cameras to target drivers in state of inebriation and the city of Bruges is testing cameras equipped with speech detection technology. De Hert, Paul & Ronny Saelens, "'Who is irritating', À propos de caméras intelligentes et d'une approche exaspérée des jeunes", *Vigiles*, 2012/2 -2012/3, pp. 267-272.

[142] See for example Haines, Alina & Helen Wells, "Persecution or protection? Understanding the differential public response to two road-based surveillance systems", supra note 1.

[143] The search is not always limited to these two databases. Some Local Police Forces for example get additional information from databases of countries surrounding Belgium, from European databases (EUCARIS), from databases of insured vehicles (VERIDASS) and other local databases (white lists and black lists).

example of ANPR cameras installed in the city centre of Oud-Turnhout to detect trucks exceeding 3,5 tonnes and of ANPR used to spot vehicles that gain unauthorised access to pedestrian areas in the city of Turnhout.[144] As for crime detection, ANPR cameras can provide information as to whether a vehicle is stolen or has been involved in crime by checking number plates against database systems of "black lists" and "white lists". Similarly, 'suspected vehicles' can be tracked and monitored. Finally, it should not be underestimated that ANPR cameras perform also the 'classical' tasks of any other CCTV camera and thus represent a valid substituted for them for law enforcement purposes.

Generally speaking, the historical development of ANPR in Belgium reflects the lack of parliamentary debate at national level and public awareness over the issue. The introduction of these systems into the daily life of Belgian citizens has not been announced by careful considerations about the need to resort to such technology, its scope and purposes. Instead, initiatives have been taken so far mostly by regional and local governments, which nonetheless have the legal autonomy to make decisions about the installation of ANPR cameras.

2. Key stakeholders

Belgium represents a very interesting and unique case study in Europe as regards the use of ANPR. This reflects to some extent the social and cultural identity/identities of the country, which is composed by the Flemish and Walloon communities. Differences in the use and deployment of ANPR can be found within the country and across regions. The Flemish-Walloon diversity plays a great role in this. In particular, differences relate mainly to the following elements:

1. Regional and local initiatives

[144] Supra note 5.

2. National government initiatives
3. Policing and regional security policies
4. Awareness about the use of ANPR systems

One can reasonably say that the Flemish region and the Brussels-capital region pioneered the introduction of ANPR in Belgium. In particular, as explained in Section 1, the first ANPR devices were installed in the province of West Flanders by the *Politiezone Westkust*. The Association of Flemish Cities and Municipalities (VVSG) estimates that half of the Flemish cities and municipalities made use of CCTV by 2011 (in public and private places). Moreover, 50 Flemish cities and municipalities (16% of Flemish cities) made use of ANPR by 2011.[145] The deployment of ANPR system in the Walloon region is even more recent. This area of the country has been endowed with ANPR devices especially at the borders with other European Member States. In fact, at present, the Walloon region is involved in experimental projects to install ANPR cameras at the border with France (see next paragraph).[146] Generally speaking, initiatives to put in place new ANPR systems and networks are proliferating in Belgium[147] and public authorities do always find new arguments to somehow legitimise these proposals. The government of Flanders for instance has recently funded a project in collaboration with the Flemish Agency for Roads and Traffic aimed at installing ANPR cameras on the region's roads.[148] In May 2013 the Walloon ministry of public works and agriculture, Carlo Di Antonio, said that he wanted to explore the

[145] VVSG, "ANPR: automatische nummerplaatherkenning, infosheet en stappenplan invoering, Infosheet en stappenplan invoering – TDS", 3 juli 2012, http://www.vvsg.be/veiligheid/camera/Documents/TDS_regelgeving%20en%20stappenplan%20ANPR.pdf (last accessed 10 December 2013).
[146] Nord Eclair, *« Wallonie Picarde : 50.000 euros pour installer des caméras de vidéosurveillance « intelligentes »»*, 1 February 2013, http://www.nordeclair.be/654969/article/regions/mouscron/actualite/2013-02-01/wallonie-picarde-50000-euros-pour-installer-des-cameras-de-videosurveillanc (last accessed 8 October 2013).
[147] See for example the recent article in the magazine of the Association of Flemish cities and municipalities (VVSG), VVSG, "Nummerplaatherkenning: niet meer telkens van nul beginnen", July 2012, http://www.vvsg.be/veiligheid/camera/Documents/Lokaal%2012%20-%20synthesenota%20vast%20anpr.pdf (last accessed 10 December 2013).
[148] Flanders Today, "Government installs ANPR cameras near Antwerp", 17 October 2013, http://www.flanderstoday.eu/current-affairs/government-installs-anpr-cameras-near-antwerp (last accessed 10 December 2013).

possibility of introducing a massive ANPR system on Walloon highways to detect those car drivers who pollute the environment throwing waste on the road and on unused areas.[149]

Apart from initiatives taken by regional and local actors, the federal government is also becoming a key stakeholder in the implementation of ANPR systems across the country. In 2012 the Belgian Ministry of the Interior, Joëlle Milquet, decided to strengthen police controls and surveillance measures at Belgian borders in order to fight against trans-border crime. 14 police districts were identified and each of them was given 50,000 euro for the purchase of ANPR cameras that have been installed on the main cross-border highways and large cities.[150] This decision marked a shift in the approach to ANPR technologies, from regionally or locally led initiatives to national initiatives. Although one cannot underestimate the significance and impact of such a decision, it is important to note that it is part of a broader securisation move taken by the government since 2002, aimed in particular at enhancing the collaboration between Belgium and France in the fight against trans-border crime.[151] The Ministry of the Interior has recently indicated that the grant given in 2012 might be renewed for 2014.

The national Parliament has only recently been involved in the debate about the use of ANPR in Belgium and until 2011 it has played a quite marginal role. So far, parliamentary debates have focused on the need to regulate ANPR technology by law and on the existing national legal framework (see Section 4).

---

[149]RTBF, *« Des caméras intelligentes pour traquer les pollueurs sur les autoroutes »,* 10 mai 2013, http://www.rtbf.be/info/belgique/detail_des-cameras-intelligentes-pour-traquer-les-pollueurs-sur-les-autoroutes?id=7991466 (last accessed 8 October 2013).

[150] As the Belgian Ministry of the Interior reports, the14 police districts are the following: Antoing / Brunehaut / Rumes / Tournai (1); Mouscron (2); Comines-Warneton (3); Celles / Estaimpuis / Mont-de-l'Enclus / Pecq (4); Bernissart / Péruwelz (5); Dour / Hensies / Honnelles / Quiévrain (6); Bilzen / Hoeselt / Riemst (7); Dilsen-Stokkem / Maaseik (8); Lanaken / Maasmechelen (9); Ledegem / Menen / Wevelgem (10); Kortrijk / Kuurne / Lendelede (11); Alveringem / Lo-Reninge / Veurne (12); De Panne / Koksijde / Nieuwpoort (13); Heuvelland / Ieper / Langemark-Poelkapelle / Mesen / Moorslede / Poperinge / Staden / Vleteren / Wervik / Zonnebeke (14). See Belgian Ministry of the Interior, Press room, "Dans la lutte contre la criminalité transfrontalière, Joëlle Milquet insiste sur l'importance du développement des caméras ANPR et ne souhaite pas réinstaurer des contrôles à la frontiere", http://www.milquet.belgium.be/fr/dans-la-lutte-contre-la-criminalit%C3%A9-transfrontali%C3%A8re-jo%C3%ABlle-milquet-insiste-sur-l%E2%80%99importance-du (last accessed 8 October 2013).

[151] Ibid.

Together with local authorities, Belgian local and federal police forces are certainly playing a crucial role in the use and promotion of ANPR. They favour initiatives aimed at intensifying the use of this technology in order to prevent, detect and combat crime. Nowadays the implementation of ANPR in Belgium is framed within the police's 'nodal orientation' doctrine. This concept refers to the surveillance of infrastructure, or rather of flows of people, goods, money and information that use the infrastructure to move from one place to another.[152] At present, ANPR is deployed mainly to combat vehicle and licence plate thefts at local level, whereas it is used to impose vehicle taxes and law enforcement purposes in general at federal and regional level. Belgian local and federal police forces are endowed with ANPR cameras that are able to scan one or more number plates in real time. In particular, once the number plate is scanned, it is searched (among other things) against the national BNG database[153] which classifies plates according to specific criteria which could consist in a mere suspicion ('geseind voertuig/*objet signalé*', targeted object) or an evidence of crime ('gestolen voertuig/*véhicules voles*', stolen vehicle). Police authorities are already appreciating the added value that this technology brings (and could bring in the future) and how ANPR footage could be better combined with the use of other technologies. Furthermore, several police districts of the country combine ANPR cameras with the software application InfoTARGET. It allows police officers to consult, match and exchange updated policing information in real time and to have them displayed on Google Maps. In particular, once information about a 'suspected vehicle' is uploaded in InfoTARGET (such as

[152] Van Ooijen, Charlotte, "Legitimacy issues regarding citizen surveillance: the case of ANPR technology in Dutch policing", in Van Der Hof, Simone & Marga M. Groothuis, *Innovating government. Normative, policy and technological dimensions of modern government*, Information Technology and Law Series, Vol. 20, Springer, 2011, pp. 197-216. De Schepper, Tom and Paul De Hert, "A descriptive review of the use of CCTV in Flemish municipalities", in Webster, William et al., *Living in surveillance societies: 'the state of surveillance'*. Proceedings of the LiSS Conference 3, 2012, pp. 145-161. Known also as 'infrastructure policing', the doctrine of 'nodal orientation' developed in Dutch-speaking municipalities first.

[153] The National General Database, Banque de données nationale générale (BNG), http://www.polfed-fedpol.be/org/org_cg_cgo_dsb_en.php "includes all the information systems of the integrated police supporting judicial or administrative police missions, in order to enable an optimal, structured and secure flow of information. It can be seen as a large box containing all the useful information about persons, vehicles, places, etc." Federal Police, Directorate of Operational Police Information, National General Database (last accessed 10 December 2013).

the number plate or vehicle registration details), it is matched against real-time location data provided by ANPR cameras. [154] The combination of ANPR cameras with InfoTARGET represents for the police an effective methodology to combat transnational crime. Police forces underline that developments in ANPR technologies should aim for this integrated approach.

Nevertheless, it is also important to note that the doctrine of nodal orientation does not constitute the only argument that it is used to defend the implementation of ANPR. More generally, the Belgian federal government is greatly involved in promoting the use of surveillance technologies by entrepreneurs and households as a crime prevention measure, such as CCTV. In 2012 the Belgian Ministry of the Interior encouraged businessmen and professionals to implement new CCTV systems in exchange for fiscal advantages and benefits.[155]

Belgium represents an interesting market for the surveillance industry, not only for companies dealing with ANPR systems, but also for internet and telecommunication operators in general. In 2008 the French company Survision installed ANPR cameras in the main 24 tunnels of Brussels. The Belgian company Blue Vision Telecom has operated ANPR cameras in the municipality of Malines. In 2010, the main Belgian telecom group, Belgacom, installed ANPR cameras in the police district of Turnhout. Companies are able to make big profit out of selling ANPR cameras. With a cost ranging from 20,000 (for a fixed camera) to 175,000 euro (for a mobile camera), the installation of ANPR does usually entail huge financial burdens. In addition to that, maintenance costs are as dizzying as the cost of ANPR devices themselves. It is reported that the city of Malines paid about 1,6 million euro

[154] Belgian Federal Police, Inforevue 3/2013, Megazine de la Police Intégrée, pp. 26-27. Available at: http://issuu.com/fedpolbelgium/docs/ir03-2013fr/27?e=4373256/5193487 (last accessed 8 October 2013).

[155] Belgian Treasury, Federal Public Service Finance, *Sécurisez vos locaux professionnels et bénéficiez d'avantages fiscaux*, http://koba.minfin.fgov.be/commande/pdf/folder-securisez-vos-locaux-professionnels-2011.pdf (last accessed 11 October 2013).

for 46 ANPR cameras and spends 72,000 euro for their maintenance every year.[156] Because of the increasing use of ANPR devices, the Belgian market is getting the attention of new private companies, like Rauwers. In 2012 the group organised a "police exchange meeting" in Brussels where many police officers gathered and were confronted with positive experiences in using ANPR technologies.[157] It is important to note that, despite the huge costs related to the implementation of ANPR schemes, companies succeed in selling ANPR cameras breaking through public authorities' resistance and scepticism. This can be partly explained by the appeal of ANPR cameras as smart gadgets on the security market. On the one hand, public authorities pretend to tackle security and law enforcement issues by increasing surveillance. On the other, private companies make pressure on public authorities through persuasive strategies, such as offering ANPR cameras in exchange for cheap utility costs.[158]

Citizen's awareness about the use of ANPR systems is low. However, the Flemish community seems to be actively involved in the debate about the use of ANPR in Belgium, more than the French-speaking community. The Flemish League of Human Rights is one of the most involved NGOs in this debate. Recently the organisation warned of the dangers and risks linked to the increasing use of ANPR systems in Belgium while addressing privacy concerns openly.[159] Every year the Flemish League grants the Big Brother Awards which identify practices or measures which violate privacy the most. Together with "Big Brother in

[156] Liga voor Mensenrechten, "Nummerplaatherkenning (ANPR)", Big Brother Awards 2013, 2013, p. 5, http://www.bigbrotherawards.be/bestanden/uploads/BBA2013_dossier_ANPR.pdf (last accessed 10 December 2013).
[157] This kinds of meetings are organised on a quite regular basis by Local Police Forces, police organisations and market players. Rauwers, "*Premier 'Police exchange meeting'. Les expériences ANPR d'outre-Atlantique*", http://www.rauwers.be/cms/images/documents/ANPR-fr/Journal%20de%20la%20Police%20-%20sept%202012.pdf (last accessed 11 October 2013).
[158] De Schepper, Tom and Paul De Hert, "A descriptive review of the use of CCTV in Flemish municipalities", in Webster, William et al., Living in surveillance societies: 'the state of surveillance'. Proceedings of the LiSS Conference 3, 2012, pp. 145-161. Liga voor Mensenrechten, "Nummerplaatherkenning (ANPR)", Big Brother Awards 2013, supra note 23.
[159] Liga voor Mensenrechten, *Mobiele camera's: vandaag voor onverzekerde voertuigen, morgen voor iedereen?*, 25 April 2013 http://www.mensenrechten.be/index.php/site/nieuwsberichten/mobiele_cameras_vandaag_voor_onverzekerde_voertuigen_morgen_voor_iedereen (last accessed 11 October 2013).

the workplace", the Belgian winner of the 2013 Big Brother Awards is ANPR. The jury of experts of the prize provided 6 main arguments to motivate its decision, namely: ANPR cameras violate privacy and the law; they entail the risk of function creep; they are not cost-effective; their installation meets commercial pressures instead of security concerns; the use of ANPR systems is hardly questioned; the use of ANPR cameras results in widespread surveillance.[160] Human rights activists of the Flemish League told us that, despite the increasing use of ANPR cameras in Belgium, ANPR did not receive as many votes as expected as candidate to the 2013 Big Brother Awards. This confirms the lack of awareness of Belgian citizens about the use of ANPR technologies, as well as general public's perceptions regarding ANPR. So far, the Walloon counterpart of the Flemish League has not taken the chance to express the same level of criticism towards the use of ANPR systems.

The Association of Flemish Cities and Municipalities, VVSG (NGO) is also playing a key role in raising awareness about the use and deployment of ANPR systems in the Flemish areas of the country. It reports constantly about developments at local and regional level which concern surveillance technologies and ANPR in particular. It has to be recognised that the bulk of the data which are currently available about the use of ANPR in Belgium have been gathered by the VVSG.

Together with civil society organisations, the Belgian DPA (hereafter the Privacy Commission) is actively involved in raising awareness and safeguarding citizen's rights in the use of ANPR technologies. The Privacy Commission has adopted a cautious approach towards the deployment and use of ANPR while ensuring compliance of such new surveillance practices with national law. Moreover, to a certain extent the Privacy Commission has had a positive approach towards ANPR. It has not resisted the deployment of fixed ANPR, but asked for a legal basis to legitimise the use of mobile ANPR devices. The peculiar role of the Belgian DPA was reaffirmed in 2012, when it issued a recommendation

[160] Liga voor Mensenrechten, Big Brother Awards 2013, http://www.bigbrotherawards.be/index.php/nl/ (last accessed 10 December 2013).

dealing with ANPR cameras (see Section 4 infra). More recently the Privacy Commission expressed some criticism with regards to ANPR and new technologies in general.[161]

3. Issues and controversies

The swift deployment of ANPR systems is originating increasing concerns. Although the Belgian lay citizen has still to realise that actually these technologies are operated in their daily lives, steps are being taken to raise awareness and more criticism towards their use and effects. As explained in Section 2, NGOs are playing a crucial role in this, with the VVSG and the Flemish League of Human Rights being very active. Given the lack of a truly public debate on the issue, civil society organisations are bringing into question the usefulness of this technology and their impact on privacy, putting forward Big Brother arguments similar to those used in the case of CCTV. From a human rights perspective it is argued that the use of ANPR entails a breach of privacy law and of the right to be presumed innocent (principle of the presumption of innocence). In addition to that, it is claimed that the deployment of ANPR violates the principle of the rule of law as at present the use of mobile ANPR devices still lacks a legal basis. The origin and consequences of this legislative void are better described in Section 4.

The six arguments put forward by the Flemish League of Human Rights on occasion of the Big Brother Awards (see above) map the issues and controversies linked to the use of ANPR in Belgium. Together with the risk of function creep, the lack of social awareness and acceptance of ANPR represents a major source of concern. Public debate about the use of ANPR has taken place only recently and in particular as of 2012 with the development of

[161] Privacy Commission, Advice no. 42/2013 of 2 October 2013 on the draft of the new camera law, "Avant-projet de la loi modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance (CO-A-2013-046) ". See also VVSG "Privacycommissie vraagt debat over camera's en drones", 28 December 2013, http://www.vvsg.be/Lists/Nieuws/dispform.aspx?id=1919&Source=http%3a%2f%2fwww.vvsg.be%2fveiligheid%2fPages%2fNieuws.aspx (last accessed 29 December 2013).

federal and regional ANPR projects. There has not been much debate before the implementation of ANPR in Belgium and decisions have been taken without public consultation. Indeed, in the early stages of the development of ANPR schemes the DPA was not even consulted. On the one hand, governmental authorities and the local and federal police forces are now encouraging the use of ANPR. They argue that these technologies provide a valuable support in dealing with road traffic offences and crime. However, explanations still have to be given about how ANPR will be used in the future and limits about the implementation of these technologies still have to be set. On the other hand, civil society organisations are fuelling the public debate raising privacy and human rights concerns which local administrators and police officers have almost disregarded so far. However, much more efforts are needed to engage Belgian citizens in the debate about the use of ANPR and to call into question the utilitarian arguments used by public authorities and companies to legitimise the use of ANPR.

4. Regulation of ANPR in Belgium

The legal framework that applies to ANPR cameras in Belgium is a vague and complex one and in the last years many doubts and concerns have been raised about the applicability of the existing legislation. The main legislative text that regulates the installation and use of ANPR in Belgium is the 2007 *Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's*/*Loi réglant l'installation et l'utilisation de caméras de surveillance* [162] (hereafter the *Camerawet*/*Loi caméras*) and its 2009 amendment.[163] In addition, the use of ANPR systems is regulated also by the Belgian Law of 1996 on the authorisation and use in road traffic of automatic devices (in particular for the metric standardisation of cameras)[164]

[162] Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007, M.B. 31 May 2007.
[163] Belgian Parliament, *Loi visant à modifier la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance*, 12 November 2009, M.B. 18 December 2009.
[164] Belgian Parliament, Law of 4 August 1996 relative to the autorisation and use in road traffic of automatic devices in presence or absence of official agent, M.B. 12 September 1996.

and the Belgian Data Protection Act.[165] The *Loi caméras* and its 2009 amendment constitute the heart of this legislative framework. As it will be explained hereafter, although the 2009 amendment clarified some of the key aspects in the regulation of ANPR cameras, ambiguities and doubts about the legality of such surveillance practice still exist.

The *Loi caméras* applies to any fixed or movable system of observation whose aim is to prevent, ascertain or detect crimes against persons or assets or offences of the same kind (Art. 2, 4°).[166] On the one hand, in 2007 the adoption of the *Loi caméras* paved the way for the specific regulation of cameras in Belgium and at last gave the country the possibility to rely on clear provisions about the installation and use of CCTV technologies. On the other, it generated doubts about the applicability of these rules to ANPR cameras. The main legal concern was linked to the fact that, as stressed earlier, ANPR were considered as *smarter* than other CCTV cameras and hence it was not clear if ANPR cameras could be automatically assimilated to *normal* CCTV cameras.[167] In particular, the 2007 *Loi caméras* did not clarify whether its provisions were applicable to mobile ANPR cameras. There were opposing interpretations and views in this regard[168] which led the Belgian legislator to amend the law while trying to solve this ambiguity. The 2009 amendment introduced the definition of mobile cameras which "allow observation from different places or positions".[169] Although the 2009 amendment made clear that the *Loi caméras* applies also to mobile cameras when

[165] Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993 (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*/*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)*.

[166] Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance,* ibid. Translation from the French "tout système d'observation fixe ou mobile dont le but est de prévenir, de constater ou de déceler les délits contre les personnes ou les biens ou les nuisances".

[167] De Hert, Paul & Ronny Saelens, "'Who is irritating', À propos de caméras intelligentes et d'une approche exaspérée des jeunes", supra note 8.

[168] On the one hand, it was claimed that the *Loi caméras* was not applicable in the case ANPR because none of its provisions mentioned this explicitly. On the other, it was argued that fixed ANPR cameras only could be installed in the framework of the Camera Act, whereas mobile ANPR cameras could not. This latter position was endorsed by the Belgian Ministry of the Interior, as stated before the federal parliament in 2009. Schriftelijke vraag nr. 112 van H. Bogaert van 28/07/2009.

[169] Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance,* ibid. The 2009 amendment established that a mobile camera is "déplacée au cours de l'observation afin de filmer à partir de différents lieux ou positions".

used on occasion of big gatherings, it did not provide any clarification about the use and installation of mobile ANPR cameras in more general contexts. In 2012 the Privacy Commission addressed this ambiguity of the *Loi caméras* in its Recommendation n. 4.[170] As the Belgian DPA confirmed,:

"*the Loi caméras establishes that the use of mobile cameras by the police is admitted only in the framework of "big gatherings" (i.e. a demonstration, a rock concert, …). The use of mobile cameras which recognise number plates in order to search for stolen vehicles, suspects, etc. is accordingly problematic, considered the recent adaptation of the Loi caméras. By contrast, according to the Loi caméras, the use of fixed surveillance cameras which recognise number plates is certainly possible and legally coherent*".[171]

Hence, provided that the *Loi caméras* applies to fixed ANPR cameras, the Belgian DPA invited the government to fix those problematic aspects related to the use of mobile ANPR cameras. Further to the DPA's recommendation, a proposal to modify the *Loi caméras* was formally submitted to the Belgian Senate on 20 June 2013.[172] This new amendment, which is pending approval, will finally make the use of mobile ANPR cameras legitimate under Belgian law. The revision of the *Loi cameras* is expected in early 2014 and lawyers look forward to a detailed legal framework for mobile ANPR and smart cameras.

---

[170] Privacy Commission, Recommendation no. 4/2012 of 12 February 2012 on the different applications of surveillance by cameras, "Recommendation d'initiative sur les diverses possibilités d'application de la surveillance par caméras".

[171] The text within inverted commas here is an unofficial translation into English of the original French document. The corresponding paragraph of the Recommendation reads as follows: "*la loi caméras prévoit explicitement que le recours à des caméras mobiles par les services de police n'est possible que dans le cadre de ce qu'on appelle des "grands rassemblements" (par ex. une manifestation, un concert rock, …). L'utilisation de caméras de surveillance mobiles avec reconnaissance des plaques d'immatriculation en vue notamment de rechercher des véhicules volés, des personnes signalées, etc. est en d'autres termes de lege lata problématique, vu cette récente adaptation de la loi caméras. Par contre, selon la loi caméras, l'utilisation de caméras de surveillance fixes avec reconnaissance des plaques d'immatriculation est bel et bien possible et juridiquement cohérente*". Privacy Commission, Recommendation no. 4/2012 of 12 February 2012, ibid., para. 53.

[172] Sénat de Belgique, "Proposition de loi modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance", déposée par MM. Guido De Padt et Yoeri Vastersavendts, Session de 2012-2013, 5-2159/1, 20 June 2013.

Debates about the proposed amendments to the *Loi caméras* have been going on in the Belgian Parliament since mid-2013. Different opinions have emerged with regards to the design of a new legal framework concerning the use of ANPR cameras by police forces. In particular, two different views opposed. On the one hand, Liberals were more inclined to integrate legal provisions concerning the use of ANPR cameras into the existing *Loi caméras.* On the other, Christian Democrats wanted to incorporate them into the Police Act.[173] Lastly, this latter position has prevailed.

5. ANPR cameras and the media

Belgian media are getting increasingly involved in the public debate over the use of ANPR technologies. News about the installation of new ANPR cameras are reported on a regular basis and journalists are somehow witnessing the rise of these new surveillance devices. Generally speaking, it is more likely to find press-related information on this subject in Flemish than in French. Accordingly, the Flemish public opinion seems to be more attentive and sensitive to the implementation of ANPR schemes. Belgian media have reported about ANPR since 2005, when this technology got the interest of public authorities. However, one can reasonably say that ANPR has hit the headlines since 2011, when ANPR-related initiatives grew in terms of quantity and importance.

Belgian media have long highlighted the added value of ANPR as smart cameras, so sharing the views of public authorities and private companies. It is quite hard to find in the press references to privacy and more generally to the impact of ANPR on fundamental rights and freedoms, although national press is now giving more attention to these aspects.[174] Similarly, arguments concerning the risk of the function-creep seem to be mainly disregarded by the

[173] Belgian Parliament, "Proposition de loi modifiant la législation relative à l'utilisation de caméras de surveillance par les fonctionnaires de police", doc.nr. 3042/001, 3 October 2013, http://www.dekamer.be/FLWB/PDF/53/3042/53K3042001.pdf (last accessed 23 December 2013).

[174] See for example De morgen, "Van trajectcontrole naar controlestaat?", 23 October 2013, http://www.demorgen.be/dm/nl/2461/Opinie/article/detail/1727720/2013/10/23/Van-trajectcontrole-naar-controlestaat.dhtml (last accessed 23 December 2013). See also the recent participation of Prof. Paul De Hert to the TV program 'VOLT', on the local channel VRT.

media. Indeed, the lack of a proper public debate on the use of ANPR is still a matter of concern. However, it is important to note that the press has mentioned about the lacunae of the national legislative framework since 2009 while envisaging amendments to the provisions of the *Loi caméras*, in particular with regards to mobile ANPR cameras.[175]

6. Accountability

The analysis developed in the previous sections let us argue that the relationship between the watcher and the watched in the implementation of ANPR schemes in Belgium is seriously unbalanced. There are different ways in which public authorities and the local and federal police forces could be made accountable for the installation and use of ANPR cameras. However, these accountability strategies seem to be ineffective at present mainly because of the weak position of the watched in comparison with the watcher. Nonetheless, the *Loi caméras* does not ask for any kind of evaluation or public accountability of a camera system. For fixed ANPR cameras a public advice of the city council is however obliged by law. In the near future, as the new *Loi caméras* will include a legal framework for mobile ANPR cameras, accountability mechanisms might be set towards the Belgian Ministry of the Interior or the council of the concerned local police force. In turn, decisions about the resort to ANPR surveillance would be somehow shifted from city councils towards higher-scale councils of local police forces which have almost no link with 'ordinary citizens'.

As illustrated in Section 2, public administrations are paving the way for the deployment of far-reaching and long-term ANPR projects in Belgium.[176] They justify ANPR schemes on the basis of arguments accompanied by rhetorics of security which are likewise endorsed by private companies. Such decisions have been taken without involving the public and the concerned citizens, while investing public money in ANPR technologies. In an ideal situation,

[175] Le Vif, Datanews, "ANPR: certains anticipent un changement de la 'loi caméras", 23 September 2009, http://datanews.levif.be/ict/actualite/anpr-certains-anticipent-un-changement-de-la-loi-cameras/article-1194716377141.htm (last accessed 11 October 2013).

[176] Indeed, the Belgian *Loi caméras* does not ask for temporary limited camera projects, which is the case in other European member states.

citizens should have been made aware about why ANPR systems were needed, which purposes the public administration wanted to reach by installing ANPR cameras and how such surveillance measure was supposed to be implemented. Similarly, citizens should have been made aware about the impact of ANPR technologies on their daily life. So far, these accountability mechanisms have failed against security rhetorics and imperatives.

7. ANPR and access requests

The exercise of access rights represents one of the ways through which citizens can make public authorities and the police accountable for the use of surveillance devices such as CCTV and ANPR cameras. This mechanism of accountability turned out to be extremely fragile when we claimed access to images about ourselves stored into ANPR cameras.[177] In this circumstance data controllers denied our access invoking, among other things, specific provisions of the above-mentioned *Loi caméras.* In particular, we found three main difficulties in having access to ANPR footage. They refer to the following aspects.

Storage period, formal requirements and data controllers' practices

In Belgium local and federal police authorities keep control of images filmed by ANPR cameras in public places. After having located the data controller, we contacted the police asking for access to images taken by an ANPR camera installed in the city centre of Brussels. We introduced a written request, according to Art. 10 of the Privacy Act.[178] First of all, the denial of our request was based on the argument that images had been erased, as police authorities store them for less than 10 days. Complying with the formal requirements

[177] This 'exercise' was undertaken in the framework of IRISS WP5 ('Exercising democratic rights under surveillance regimes'). For a more detailed analysis of access rights in Belgium, see the IRISS deliverable issued from WP5.

[178] According to Art. 10 of the Privacy Act, "the data subject shall submit a signed and dated request to the controller (…). The information shall be communicated without delay, at the very latest forty-five days after receipt of the request". Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993 (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*/*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)*.

prescribed under Belgian law, our request was sent by post and it took a couple of days to be notified by the police. In turn, the police took several days to come back to our request (indeed, data controllers can take forty-five days to reply to the data subject, according to Art. 10 of the Privacy Act). As a consequence, formal and procedural requirements turned our demand into a void request. It is important to note that, as this example suggests, the right of access to ANPR images is substantially left to the discretionary power of the data controller.

Motivation

Art. 12 of the *Loi caméra* establishes that everyone who has been filmed has the right to access images that concern him/her. In order to do so, it is necessary to submit a written and motivated[179] request to the data controller. Data controllers consider a suitable motivation to be a notice of crime or an event that threatens public security which has been reported to the police. Our access request was not linked to any of these two situations, hence the police rejected our request.

Data sharing

Thirdly, the police refused to grant access to ANPR images arguing that they share footages on the basis of an official statement of offence, a formal indictment of judicial authorities or an order of the crown prosecutor only.

8. Resilience

As illustrated earlier, one can identify two key moments in the history of ANPR in Belgium. From 2005 to 2012 the implementation of ANPR schemes consisted mainly in small-scale initiatives and pilot projects set at local level. Since 2012, there has been a significant increase in the use of ANPR devices across the country, with the substantial engagement of

[179] The Privacy Commission underlines that the request has to be “dûment motivée” (duly motivated).

the Belgian federal and regional governments. Framed in terms of stresses and shocks (see IRISS Deliverable 6), one can reasonably argue that resilient attitudes have emerged since 2011, when ANPR initiatives proliferated in terms of quantity and importance. However, it is hard to say that the Belgian society is or is becoming resilient towards the use of ANPR cameras nowadays. As explained in Section 2, substantial differences can be found within the country and at regional level, which of course have a great impact on the way citizens respond to such surveillance moves. Taking into account the replies of our respondents, we can say that Belgian citizens need to become more aware about the use of ANPR devices in order to increase their resilience towards ANPR technologies. The lack of resilience of Belgian citizens towards ANPR and surveillance cameras in general is also confirmed by the results of the recent national empirical research on public cameras in Belgium.[180]

Indeed, the lack of awareness represents to a certain extent an obstacle towards the development of a resilient behaviour. Some of our respondents for example said that they do not like being under the gaze of ANPR cameras but they cannot really avoid it. One cannot escape ANPR-related checks when crossing the Belgian border. Similarly, drivers cannot divert their route only because there are ANPR devices in operation on a certain highway. Most of all, given the recent use of ANPR systems in Belgium, drivers do not know where and when they will be subject to checks performed by mobile ANPR cameras.[181] Being against the principle of foreseeability (Art. 8.2 of the European Convention on Human Rights), this proves that the implementation of many ANPR schemes might fail privacy checks.

[180] Mortelé, Jill, Hans Vermeersch, Evelien De Pauw, Wim Hardyns, Famke Deprins, "Cameratoezicht in de openbare ruimte. Ook wie weg is, is gezien?", Maklu 2013, Reeks Politiestudies, nr. 6.
[181] By contrast, the operation of fixed ANPR cameras is announced by on-site pictogrammes according to the *Loi caméras*.

Conclusion

Apart from the detection of traffic offences, in principle ANPR could have many more applications in the future and be used to detect any crime committed with help of a vehicle. It is more than realistic to foresee that ANPR could be used to track and monitor individuals and that ANPR evidence (that is the results of a registration by ANPR cameras) could be brought before courts in the near future. If so, ANPR would prove to be a smart surveillance technology able to combine visual data with location data. From the local and federal police forces and public authorities' perspectives it would certainly become more reliable and effective than GPS or mobile tracking technologies. Of course, these future scenarios raise several concerns. Many of them are linked to the so-called function creep. It is important here to note that, as illustrated in this paper, these concerns are not only legal (leading to the infringement of the right to privacy, the right to be presumed innocent and possibly in the near future the right to be forgotten) but they also involve more broadly the policy sphere touching upon the values of accountability and transparency.

Among other things, this report illustrated how the use of a new surveillance technology can result in a truly unbalanced relationship between the watcher and the watched. In other words, this shows how the watched is being marginalised not only when accessing the technology itself but also when accessing data and information stored into ANPR systems. Lack of awareness, bureaucratic processes, and more traditional *raison d'état* arguments create that unbalance between the watcher and the watched, while making rhetorics of security prevail over human rights.

Bibliography

Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993.

Belgian Parliament, Law of 4 August 1996 relative to the autorisation and use in road traffic of automatic devices in presence or absence of official agent, M.B. 12 September 1996.

Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007, M.B. 31 May 2007.

Belgian Parliament, *Loi visant à modifier la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance*, 12 novembre 2009, M.B. 18 December 2009.

De Hert, Paul & Ronny Saelens, "'Who is irritating', À propos de caméras intelligentes et d'une approche exaspérée des jeunes", *Vigiles*, 2012/2 -2012/3, pp. 267-272.

De Schepper, Tom and Paul De Hert, "A descriptive review of the use of CCTV in Flemish municipalities", in Webster, William et al., Living in surveillance societies: 'the state of surveillance'. Proceedings of the LiSS Conference 3, 2012, pp. 145-161.

De Schepper, Tom (eds.), *Praktijkgids Cameratoezicht*, VVSG-Politeia, Brussels, 2013.

Haines, Alina & Helen Wells, "Persecution or protection? Understanding the differential public response to two road-based surveillance systems", *Criminology and Criminal Justice*, Sage, Vol. 12, No. 3, pp. 257-273.

Mortelé, Jill, Hans Vermeersch, Evelien De Pauw, Wim Hardyns, Famke Deprins, "Cameratoezicht in de openbare ruimte. Ook wie weg is, is gezien?", Maklu 2013, Reeks Politiestudies, nr. 6.

Parsons, Christopher, Joseph Savirimuthu, Rob Wipond and Kevin McArthur, “ANPR: code and rhetorics of compliance”, *European Journal of Law and Technology*, Vol. 3, No. 3, 2012.

Privacy Commission, Recommendation no. 4/2012 of 12 February 2012 on the different applications of surveillance by cameras, “Recommendation d’initiative sur les diverses possibilités d’application de la surveillance par caméras”.

Privacy Commission, Advice no. 42/2013 of 2 October 2013 on the draft of the new camera law, “Avant-projet de la loi modifiant la loi du 21 mars 2007 réglant l’installation et l’utilisation de caméras de surveillance (CO-A-2013-046) ”.

Sénat de Belgique, “Proposition de loi modifiant la loi du 21 mars 2007 réglant l’installation et l’utilisation de caméras de surveillance”, déposée par MM. Guido De Padt et Yoeri Vastersavendts, Session de 2012-2013, 5-2159/1, 20 June 2013.

Van Der Hof, Simone & Marga M. Groothuis, *Innovating government. Normative, policy and technological dimensions of modern government*, Information Technology and Law Series, Vol. 20, Springer, 2011, pp. 197-216.

Webster, William et al., *Living in surveillance societies: ‘the state of surveillance’*. Proceedings of the LiSS Conference 3, 2012, pp. 145-161.

Online sources

Belgacom, ICT News, *La Police vous voit*, *Les lecteurs de plaques minéralogiques améliorent la sécurité*, 24 September 2010, http://www.ictnews.be/fr/2010/09/24/the-police-are-watching/ (last accessed 8 October 2013).

Belgian Federal Police, Inforevue 3/2013, Megazine de la Police Intégrée, pp. 26-27. Available at: http://issuu.com/fedpolbelgium/docs/ir03-2013fr/27?e=4373256/5193487 (last accessed 8 October 2013).

Belgian Ministry of the Interior, Press room, "Dans la lutte contre la criminalité transfrontalière, Joëlle Milquet insiste sur l'importance du développement des caméras ANPR et ne souhaite pas réinstaurer des contrôles à la frontiere", http://www.milquet.belgium.be/fr/dans-la-lutte-contre-la-criminalit%C3%A9-transfrontali%C3%A8re-jo%C3%ABlle-milquet-insiste-sur-l%E2%80%99importance-du (last accessed 8 October 2013).

Belgian Treasury, Federal Public Service Finance, *Sécurisez vos locaux professionnels et bénéficiez d'avantages fiscaux*, http://koba.minfin.fgov.be/commande/pdf/folder-securisez-vos-locaux-professionnels-2011.pdf (last accessed 11 October 2013).

Blue Vision Telecom, *ANPR Project Mechelen*, 2011, http://www.bluevisiontelecom.be/news/anpr-project-mechelen (last accessed 8 October 2013).

De morgen, "Van trajectcontrole naar controlestaat?", 23 October 2013, http://www.demorgen.be/dm/nl/2461/Opinie/article/detail/1727720/2013/10/23/Van-trajectcontrole-naar-controlestaat.dhtml (last accessed 23 December 2013).

Flanders Today, "Government installs ANPR cameras near Antwerp", 17 October 2013, http://www.flanderstoday.eu/current-affairs/government-installs-anpr-cameras-near-antwerp (last accessed 10 December 2013).

Gouvernement de la région Bruxelles-capitale, press realease, *« Premier radar équippé d'une caméra*

Le Vif, Datanews, "ANPR: certains anticipent un changement de la 'loi caméras", 23 September 2009, http://datanews.levif.be/ict/actualite/anpr-certains-anticipent-un-changement-de-la-loi-cameras/article-1194716377141.htm (last accessed 11 October 2013).

Liga voor Mensenrechten, "Nummerplaatherkenning (ANPR)", Big Brother Awards 2013, 2013, p. 5, http://www.bigbrotherawards.be/bestanden/uploads/BBA2013_dossier_ANPR.pdf (last accessed 10 December 2013).

Liga voor Mensenrechten, *Mobiele camera's: vandaag voor onverzekerde voertuigen, morgen voor iedereen?*, 25 April 2013 http://www.mensenrechten.be/index.php/site/nieuwsberichten/mobiele_cameras_vandaag_voor_onverzekerde_voertuigen_morgen_voor_iedereen (last accessed 8 October 2013).

Nord Eclair, *« Wallonie Picarde : 50.000 euros pour installer des caméras de vidéosurveillance « intelligentes »»*, 1 February 2013, http://www.nordeclair.be/654969/article/regions/mouscron/actualite/2013-02-01/wallonie-picarde-50000-euros-pour-installer-des-cameras-de-videosurveillanc (last accessed 8 October 2013).

Politiezone Westkust, "Persmap Politiezone Westkust", 13 December 2013 http://www.lokalepolitie.be/sites/5461/images/teksten/persbabbel%2013%20december%202013.pdf (last accessed 23 December 2013).

Rauwers, "*Premier 'Police exchange meeting'. Les expériences ANPR d'outre-Atlantique*", http://www.rauwers.be/cms/images/documents/ANPR-

fr/Journal%20de%20la%20Police%20-%20sept%202012.pdf (last accessed 11 October 2013).

Rauwers, *Reportage RTL-TVI*, *ANPR Voiture Scanner à Liège*, 16 January 2012, http://www.rauwers.be/cms/index.php/fr/the-news/150-anpr-reportage-rtl-tvi (last accessed 8 October 2013).

RTBF, *« Des caméras intelligentes pour traquer les pollueurs sur les autoroutes »,* 10 mai 2013, http://www.rtbf.be/info/belgique/detail_des-cameras-intelligentes-pour-traquer-les-pollueurs-sur-les-autoroutes?id=7991466 (last accessed 8 October 2013).

Survision, *Press Releases*, June 2008, Brussels, http://www.survision.fr/press/PR_2008_06_25.php (last accessed 8 October 2013).

VVSG, "Nummerplaatherkenning: niet meer telkens van nul beginnen", July 2012, http://www.vvsg.be/veiligheid/camera/Documents/Lokaal%2012%20-%20synthesenota%20vast%20anpr.pdf (last accessed 10 December 2013).

VVSG, "ANPR: automatische nummerplaatherkenning, infosheet en stappenplan invoering, Infosheet en stappenplan invoering – TDS", 3 juli 2012, http://www.vvsg.be/veiligheid/camera/Documents/TDS_regelgeving%20en%20stappenplan%20ANPR.pdf (last accessed 10 December 2013).

VVSG "Privacycommissie vraagt debat over camera's en drones", 28 December 2013, http://www.vvsg.be/Lists/Nieuws/dispform.aspx?id=1919&Source=http%3a%2f%2fwww.vvsg.be%2fveiligheid%2fPages%2fNieuws.aspx (last accessed 29 December 2013).

1. ANPR GERMANY

Kerstin Goos, Sebastian Dahm, Michael Friedewald

1.1 INTRODUCTION

In Germany, Automatic Number Plate Recognition (ANPR) is applied in four main use areas: first, as a support tool for police work – for crime prevention and law enforcement; second, to collect data for the purpose of checking if trucks are paying the correct tolls; third, ANPR can also be applied as part of a building's security system, e.g. in order to control whether a vehicle may enter a specific area; fourth, for traffic management, e.g. to count the number of cars driving on a specific street.

Of these four applications, two are worthy of particular study – police work and toll control. These two use areas are the most important in terms of frequency of use, controversy and public debate surrounding the topic. This contribution aims at investigating ANPR in Germany, with a focus on identifying how, and whether, democratic activities feature within this surveillance practice. As far as possible, we do this from the perspective of the watcher and the watched. The following table offers a brief overview of the two analysed applications. The table compares the watcher, the watched, the purpose of the use of ANPR, the respective system and the databases the data is matched with.

Table 1: Overview of the two analysed ANPR applications in Germany

	ANPR	
	Police work	**Toll control**
The watcher	State/police	Private company (supervised by a state authority)
The watched	Vehicles	Vehicles
Purpose	Crime prevention/law enforcement	Toll control
ANPR system	From a technical view the control related data is comparable to the data used in police work	
Databases that are matched	Tracing files	Journey related data
Scale	Between 0 and 20 devices per *Land*	300 gantries all over Germany, used in random mode

In relation to the use of ANPR for law enforcement and crime prevention, police forces are the executive power while parliaments (both on the national and the state level) decide on the legal basis and amendments. Those who are watched are the car drivers passing by the ANPR device, and the databases that are matched with the data collected via ANPR are tracing files of different types. In relation to the second application, Toll Collect GmbH, a private company that has been assigned to organise the collection of the truck toll, matches the collected data with the journey related data stored in the toll system in order to randomly control whether the toll has been paid. From a technical point of view, both systems are comparable. In practice, it is currently not allowed to use the toll infrastructure – 300 gantries all over Germany – for law enforcement. Nevertheless, discussions about, and demands for, the abolition of the purpose limitation arise regularly.

This case study is structured as follows: At first, we give a brief description of our methodology. Following this, the next part gives an overview of the two ANPR applications and is split into two: the first describes the history, regulation and implementation practice of ANPR for police work; the second illustrates similar aspects for the use of ANPR for toll control. In the three consequent chapters, we examine how, where and when it has been referred to in the German press, and, based on the media analysis, the key stakeholders and controversies. Finally we discuss our findings, ending with a conclusion.

1.2 METHODOLOGY

ANPR is a topic that has not been investigated in-depth in the German context. Sound scientific literature is rare. The most elaborated debates about ANPR have taken place in legal circles where the constitutionality of the provisions for ANPR has been a topic of discussion since the early 2000s.[182] Therefore, besides drawing on legal literature

[182] See for instance: Arzt, Clemens, "Rechtsfragen der automatisierten Kennzeichenerkennung", *Straßenverkehrsrecht*, Vol. 4, No. 9-10, 2004, pp. 368-373, 368-373; Martinez Soria, José, "Grenzen

(especially two extensive dissertation projects that examined ANPR in Germany[183]) our desk research aims to retrace political debates and actual implementations based on newspaper articles, online resources, parliamentary documentations and the *Länder* Data Protection Authorities' annual reports.

In addition, we conducted a media analysis in which we analysed public debates, stakeholders and controversies. In order to analyse how, where and when ANPR has been referred to in the German news; we decided to conduct a media content analysis. Pragmatism demands we limit our scope somewhat and our content analysis is limited to the German press.

Further information sources were qualitative, semi-structured, interviews with representatives of either the police forces or the Ministries of the Interior of the *Länder*. The interviews were based on a short questionnaire with which we aimed at understanding the implementation practice in Germany. We approached the person responsible either directly or through the ministries' general contact address. 15 – out of the 16 contacted – ministries cooperated and offered information about the implementation practice. It should be noted that some ministries offered more detailed information than others. In the analysis of the interview data, we will not refer to specific *Länder*. The interviews were conducted via telephone; if no interview was possible; questions were asked and answered in extensive email exchanges. Besides the above, 2 interviews with researchers in the field were held.

---

vorbeugender Kriminalitätsbekämpfung im Polizeirecht: Die automatisierte Kfz-Kennzeichenerkennung", *Die Öffentliche Verwaltung 18*/2007, pp. 779-785; Guckelberger, Annette, "Zukunftsfähigkeit landesrechtlicher Kennzeichenabgleichsnormen", *Neue Zeitschrift für Verwaltungsrecht*, Vol. 28, No. 6, 2009, pp. 352-358.

[183] Gasch, Patrick, *Grenzen der Verwertbarkeit von Daten der elektronischen Mauterfassung zu präventiven und repressiven Zwecken*, Duncker & Humblot, Berlin, 2012; Kenzel, Brigitte, *Die automatische Kennzeichenfahndung. Eine neue Überwachungsmaßnahme an der Schnittstelle zwischen präventivem und repressivem Einsatz*, Verlag Dr. Kovaĉ, Hamburg, 2013.

1.3 ANPR USED BY THE POLICE

Since police law is a competence of the *Länder,* and the application of ANPR is partly based on police law, each of the 16 *Länder* has its own history of ANPR (see section 1.3.3 for a detailed overview). Some have never used ANPR, some have stopped using it and some still use it. Currently, 11 *Länder* have specific regulations covering ANPR. Nevertheless, not every *Land* that adopted particular provisions for ANPR, applies those provisions. In turn, other *Länder* both have provisions that are of questionable constitutionality and apply them.

1.3.1 History of ANPR applied for law enforcement and crime prevention

The first ANPR trials in Germany took place in 2002, when Bavaria tested ANPR at the Bavarian-Czech border for the purpose of speed control and criminal prosecution[184]. Brandenburg followed: conducting a trial in 2003, although plans to use ANPR in Thuringia were stopped after intense political discussions. The first enabling provision dealing especially with ANPR was introduced in Rhineland-Palatinate in 2004. Hesse followed later in 2004 and in 2005 Hamburg also enacted regulation on ANPR.[185] In 2006 Bavaria, Brandenburg, Mecklenburg-Western Pomerania and Bremen adjusted their police laws, Schleswig-Holstein and Saarland followed in 2007. Lower Saxony adopted regulations in the beginning of 2008. The main reason for the introduction of ANPR in the different *Länder* was the promise that it would lead to increased efficiency in police work. This accounts for the use of ANPR on highways that function as transport routes for human or drug trafficking.

A milestone for ANPR regulations in Germany was the decision of the Federal Constitutional Court in March 2008. In reaction to a constitutional complaint, the prerequisites for the regulations and implementation of ANPR were clearly stated and the police laws in Hesse

[184] Arzt, 2004.
[185] Kenzel, 2013.

and Schleswig-Holstein were declared unconstitutional. After the Court decision, Hesse, Bavaria, Hamburg, Rhineland-Palatinate and Lower Saxony consequently revised their police laws; Schleswig-Holstein and Bremen voided their regulations. Those *Länder*, which had no regulation before the decision, but have since introduced such regulations, are Baden-Württemberg (in June 2008), Thuringia (July 2008) and Saxony (in 2011).

1.3.2 The system

ANPR in Germany is applied either with fixed cameras, partly fixed cameras or mobile cameras. If ANPR is used for crime prevention, the cameras are connected to a system that contains files where number plates are listed that are searched for. For instance, the police keep lists of stolen vehicles and their number plates, of tracing files and of people who are marked for observation. All these lists may contain number plates, data about the vehicle owner or the vehicle. In principle, it is possible to match all those data with the scanned number plates.[186] What kind of data is fed into the system differs between the *Länder*. Brandenburg for instance compiles a specific database for each case. In contrast, Bavaria uses already existing databases such as INPOL[187] and SIS[188]. ANPR can either be used covertly or overtly. In practice, this also differs between the *Länder* and is dependent on the specific regulations of their respective police laws.

After the system is in place, each vehicle that drives past a camera is photographed and the number plate is extracted and transformed into a combination of letters and numbers. This combination is matched with the tracing files. If a hit occurs, the responsible authority receives a signal. Then the picture that has been taken is matched manually with the tracing

[186] Roßnagel, Alexander, *Kennzeichenscanning - Verfassungsrechtliche Bewertung*, ADAC e.V., München, 2008.
[187] INPOL or INPOL-neu, as it is called since 2003, is the information system of the national police and the police forces of the *Länder* in Germany.
[188] SIS (Schengen Information System) is a governmental database used by European countries to exchange information about individuals.

file to assure that the system has correctly recognised the scanned number plate. In case of a non-hit – according to the Constitutional Court's decision – the collected data has to be deleted immediately. If ANPR is deployed for observations whose legal basis can be found in the Code of Criminal Procedure, the pictures of the number plate and related data can be stored for specific purposes under specific prerequisites that are regulated in the Code of Criminal Procedure.

1.3.3 Regulation of ANPR for crime prevention and law enforcement

Due to several reasons, the situation in Germany is rather complex. First, the legal basis, on which ANPR operates, is multi-layered. This means that ANPR operation may simultaneously fall under a number of spheres of competence and may be supervised by a number of different authorities. Since ANPR can be applied either for crime prevention or law enforcement, the legal basis can be found in the police laws of the *Länder* or in the Code of Criminal Procedure (*StPO*, *Strafprozessordnung*) that falls under the responsibility of the federal government. In the latter case the police invokes §§100h, 111, 163e, 163f StPO. And in the former case, when it comes to the deployment of ANPR for the purpose of preventing crime, the legal basis can be found in the different police laws of the *Länder*. [189]

Second – and this point is closely related to the first – the prerequisites for a deployment of ANPR differ depending on the legal basis that is invoked. When the police use ANPR based on the police laws, the procedure actually reflects an automated search for specific number plates (*automatische Kennzeichenfahndung*, meaning an automatic number plate search). Number plates are scanned and immediately matched with tracing files. If a hit occurs the respective action is initiated, if no hit occurs, all collected data is immediately deleted. These

[189] If the police uses ANPR for law enforcement (as they do) concurrent legislative competences with the Federal authorities exist. Since this would go beyond the scope of this case study, we will not analyse these discussions in detail. For further information see e.g., Guckelberger, 2009; Kenzel, 2013; Roßnagel, 2008.

strict regulations are a direct result of the decision of the Constitutional Court in 2008. The police use ANPR for several purposes such as: the search for stolen number plates or vehicles, the search for criminals or the detection of car holders that violate the obligation to have liability insurance.

As opposed to this, when the police use ANPR based on the Code of Criminal Procedure, they are allowed to either use it for an automatic number plate search or as a tool to arbitrarily scan all vehicles driving by with the aim of saving vehicle related data to process it as and when required. This practice is mostly used for observations[190] (*Kfz-Massenscanning* or *automatische Nummernschilderfassung*, meaning automatic number plate recording). Contrary to the police laws, ANPR is not explicitly regulated in the Code of Criminal Procedure. Instead, the Code of Criminal Procedure that regulates the conditions under which checkpoints aimed at the identification and detection of criminals may be put in place. Furthermore the use of technical devices for observations is regulated. Thus, the Code of Criminal Procedure offers sufficient enabling provisions for the use of ANPR for observations in specific cases of considerable importance.[191] As we will see later, the facts show that this only happens rarely.

A third factor that serves to complicate the regulatory situation in Germany is that claims against provisions in four *Länder* are currently still pending. Accordingly, the constitutionality of these regulations remains uncertain. Claims against provisions in Lower Saxony[192], Bavaria, Hesse[193] and Baden-Württemberg[194] had been lodged following the Federal Constitutional Court's decision on provisions in Schleswig-Holstein and Hesse.

[190] Kenzel, 2013.
[191] Ibid.
[192] BVerfG 1 BvR 1443/08
[193] BVerfG 1 BvR 3187/10
[194] BVerfG 1 BvR 2795/09

In other countries, permanent scanning of vehicles is deployed for a number of different purposes – such as speed control, the surveillance of parking areas or the detection of drug runners. In Germany, this is solely the case for long-term observations, and only in specific cases of particular importance.[195] Hence, the most widespread application is the matching of scanned number plates with tracing files to detect number plates or car holders listed in those files. Since ANPR falls under police law, a closer look at the respective provisions is an important step toward gaining insight into the regulation of ANPR in Germany.

When analysing the legal basis and practice of ANPR in Germany, three questions must be answered:

1. What is the legal basis a *Land* refers to in case of applying ANPR? Is there a legal basis for ANPR in the police laws of the *Länder*?
2. Are these regulations consistent with the constitution?
3. Which *Land* actually uses ANPR?

The first two questions will be answered in the next sections, and the third question in the section 1.3.4.

Specific regulations for ANPR can be found in 11 police laws (see Table 2). Berlin has no specific regulation but uses ANPR and refers to other provisions, and North Rhine-Westphalia and Saxony-Anhalt have never had regulations dealing specifically with ANPR. In Schleswig-Holstein, regulations existed between April 2007 and April 2009, when it was decided to suspend the regulations as a consequence of the Constitutional Court's decision.

[195] Kenzel, 2013.

Up to now, no new regulation has been introduced. The same accounts for Bremen, where a specific regulation existed between March 2006 and July 2008.

Table 2: Legal provisions for ANPR

Land	Specific provision for ANPR?	Where?	Since when does the current regulation exist?	Use ?
Baden-Württemberg	Yes	§22a PolG	2008	No
Bavaria	Yes	Art.33 para. 2, p.2-5, Art.38, para. 3, Art. 46, para. 2, p. 4 PAG	2008	Yes
Berlin	No	-	Police refers to other provisions	Yes
Brandenburg	Yes	§36a BbgPolG, §100 h StPO	2006	Yes
Bremen	No	Regulation existed between 2006 and 2008	-	No
Hamburg	Yes	§8a HmbPolDVG	2012	No
Hesse	Yes	§14aHSOG	2009	Yes
Lower Saxony	Yes	§32, para. 5 Nds. SOG; §§100h StPO, §111StPO in conjunction with §163 d StPO.	2009	Yes
Mecklenburg-Western Pomerania	Yes	§43a SOG-M-V in conjunction with §47 para. 2 SOG M-V, §18 para. 1 DSG M-V.	2006	Yes
North Rhine-Westphalia	No	-	Police refers to StPO	Yes
Rhineland-Palatinate	Yes	§27 para. 5 p.1 RhPfPOG	2011	n/a
Saarland	Yes	§ 27 para. 3, SaarlPolG	2007	No
Saxony	Yes	§19a SächsPolG	2011	Yes
Saxony-Anhalt	No	-	-	No
Schleswig Holstein	No	Regulation existed between 2007 and 2009	-	No
Thuringia	Yes	§33 para. 7 in conjunction with § 14 para. 1 Nr. 2 - 4 ThürPAG	2008	No

Source: Own illustration.

Crucial to the legal assessment is the question as to whether ANPR infringes upon fundamental rights, and if so, under which conditions this would be proportionate. The right that is of particular relevance in the German context is the right to informational self-determination (*Recht auf informationelle Selbstbestimmung*).[196]

The right to informational self-determination is a right that is not explicitly anchored in the German constitution, but is derived from another fundamental right, the *allgemeine Persönlichkeitsrecht*.[197] It is rooted in a judgement that passed in 1983, the so-called *Volkszählungsurteil*.[198] In this judgement, it was decided that the *allgemeine Persönlichkeitsrecht* also protects the right of the individual to decide when, and within which boundaries, personal information is disclosed.[199] The right to informational self-determination is supposed to protect the right to decide about the use of personal data in the face of developments in information technology and the new possibilities they threw up in the collection, storage and processing of data.

The practice of ANPR infringes upon the right to informational self-determination as soon as the collected data is stored. If the data is deleted immediately, for example in case of a non-hit, no intervention in the right to informational self-determination is perceived.[200] Drawing on the decision of the Federal Constitutional Court in 2008, the following aspects are prerequisites for the regulation of ANPR in the police laws (or, to put it in another way, the

[196] Kilchling, Michael and Brigitte Kenzel, "Recht und Praxis der anlassbezogenen automatischen Kennzeichenfahndung, Verkehrsdatenabfrage und Mobilfunkortung zur Gefahrenabwehr in Brandenburg. Wissenschaftliche Begleitforschung zu den §§ 33b Abs.3, Abs. 6 Satz 2 und 36a BpgPolG", Gutachten, Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2011.
[197] Art.2 par.1 in conjunction with Art.1 par.1 GG
[198] BVerGE 65, 1.
[199] BVerGE 65, 42.
[200] Kenzel, 2013. BVerfGE 120, 378 11.03.2008, para.68.

conditions under which an intervention in the right to informational self-determination is acceptable):

- Sufficiently precise enabling provisions for the respective measure are necessary, i.e. occasion, purpose and limits of the use of ANPR have to be stated clearly.[201]
- If ANPR is applied, it has to be proportionate, i.e. the enabling provisions have to take account the different uses of ANPR and their respective degrees of intervention. The degree of intervention depends on several factors; such as the occasion and the amount of data collection, the affected group of people and the intended use of the collected data.[202]

According to two comprehensive studies which investigated the constitutionality of the police laws[203], some provisions are at least questionable in terms of constitutionality. In those two studies, the different provisions are systematically investigated by referring to the above-mentioned prerequisites. Some *Länder* met the requirements in large parts, some needed improvement, and some were not compatible with the constitution.

1.3.4 Implementation

In order to be as precise and up to date in the overview of the practice of ANPR in Germany, we contacted all 16 Ministries of the Interior and asked for information via e-mail and telephone interviews about the practice of ANPR in each *Land*. Since the willingness to provide information and the comprehensiveness of the information varied, we also drew on literature reviews and parliamentary documentation. By doing this, we gained an overview of the implementation practice in Germany.

[201] BVerfGE 120, 378.
[202] Ibid.
[203] The analysis of Roßnagel (2008) was conducted before the Court decision in October 2007. Roßnagel (2009) reviewed the provisions in April 2009. The investigation of Kenzel (2013) is based on the legal situation in December 2010.

11 of the 16 *Länder* possess ANPR devices. The number of devices nevertheless varies between one and 25. All in all, the police in Germany possess approximately 70 devices. Of those which possess ANPR devices, 9 *Länder* use them for different purposes. 4 *Länder* do not use them, although legal provisions exist. As a reason for not using them one *Land* mentions that a software update is currently pending, another one lists general concerns. In another *Land,* legal provisions still exist, but the coalition agreement of the current election period envisages a suspension of the regulation. Schleswig-Holstein, whose regulation was declared unconstitutional in 2008, decided not to use ANPR anymore because of an imbalance between effort and output.[204]

Those *Länder* which decided to use ANPR name the following main use contexts: danger to life and limb (e.g. in case someone is suicidal), crime prevention in the “rocker milieu”, search for suspects before big events, control of border criminality (e.g. vehicle and property crime)[205] and the search for stolen number plates or the place of residence of a person. In addition, number plates are searched in case of a violation of the obligatory insurance law or if an arrest warrant has been issued.[206] In relation to law enforcement, ANPR is applied repressively in relation to vehicle theft and manhunts.[207]

[204] Landesregierung Schleswig-Holstein, "Automatisierte Kennzeichenerfassung nichtig – Innenminister Lothar Hay: Urteil ist Mahnung und Auftrag zugleich", Press Release, 11 March 2008.
[205] Brandenburgisches Ministerium des Innern, "Fünfter Bericht des Ministers des Innern an den Ausschuss für Inneres des Landtages über bestimmte Maßnahmen der Datenerhebung auf Grund des Brandenburgischen Polizeigesetzes", Potsdam, 2012.
[206] Landesregierung Niedersachsen, "Antwort der Landesriegierung auf die Kleine Anfrage der Abgeordneten Johanne Modder, Klaus-Peter Bachmann, Heiner Bartling, Karl-Heinz Hausmann, Jürgen Krogmann, Sigrid Leuschner, Jutta Rübke und Ulrich Watermann (SPD)", Drucksache 16/2386 neu, Niedersächsischer Landtag, Hannover, 2010.
[207] Brandenburgisches Ministerium des Innern, 2012.

For the most part, police forces use ANPR in tracing mode, which means that the aim of the implementation of ANPR is to find specific suspects.[208] Nevertheless, ANPR is also used occasionally in recording mode – although very rarely. A rather interesting case occurred in 2013, when it became public that the Federal Criminal Police Office used ANPR in an observation mode. Since 2008 the police had been searching for a criminal who randomly shot at trucks and cars on highways. In order to find the perpetrator, the police scanned all vehicles driving on specific streets, and saved the data for 10 days since December 2012. If a shot was recorded, the police matched the data with other vehicles driving in the area the crime took place.[209] According to the Federal Criminal Police Office, the use of ANPR was integral to the conviction of the perpetrator.[210] Also, it was stated that this was the first time that ANPR had been implemented on a national scale.[211] The fact that ANPR was used was only communicated after its successful use.

The situation in two *Länder* is particularly interesting: Bavaria and Brandenburg. Bavaria is an interesting case as it possesses the highest number of ANPR devices. Also, a constitutional complaint has been pending since 2008 and during the years of hearings various facts about the use of ANPR in Bavaria have become public. Brandenburg is notable as it is often referred to as a positive example and rather unique in terms of its reporting procedures that aim at transparency.

---

[208] For instance, between 2 December 2010 and 30 June 2013, the police in Hesse deployed ANPR 1241 cases in a tracing mode. In this time period 4,309,526 number plates were matched with tracing lists, and 1446 hits occurred. Based on those hits, 41 vehicles seized. See: Hessischer Minister des Inneren und für den Sport, "Antwort des hessischen Ministers des Innern und für Sport auf die kleine Anfrage des Abg. Jürgen Frömmrich (BÜNDNIS 90/DIE GRÜNEN) betreffend Einsatz von Kennzeichenlesegeräten in Hessen", Drucksache 18/7590, Hessischer Landtag, Wiesbaden, 2013.

[209] "Autobahn-Schütze handelte aus "Frust"", *Tagesschau.de*, 25 June 2013.

[210] Bundeskriminalamt, "Bundesweite Serie von Schüssen auf Autotransporter: Pressekonferenz anlässlich der Festnahme eines Tatverdächtigen", Press Release, 25 June 2013.

[211] Landesbeauftragten für den Datenschutz Rheinland-Pfalz, "Offene Datenschutzfragen im Ermittlungsverfahren gegen den Autobahnschützen ", Press Release, 25 June 2013.

Bavaria

Bavaria owns 25 ANPR devices, of which 22 are fixed devices and three are mobile devices.[212] The first pilot tests were conducted in 2002 as a reaction to the events of 9/11 and part of a counter-terrorism strategy. On the occasion of the soccer world championship in 2006, the visit of the pope in 2006[213], the Oktoberfest in 2009 and for prevention of terrorist attacks before national parliamentary elections, several devices were used. Usually the devices were installed close to the border and were permanently in operation. In case of a big event, ANPR is also temporarily deployed close to venues in order to check if a suspect is approaching. If a number plate is matched with tracing files, police forces are immediately on site to check the vehicle. ANPR in Bavaria is usually done covertly.

The geographical position and the traffic infrastructure are important rationale for the necessity of ANPR in Bavaria. Because of these, human trafficking, smuggling, arms trafficking and the illegal movement of stolen goods are of specific concern. Although the police do not keep any statistics, they see ANPR as an effective and necessary tool that is of great benefit to their work.

When it comes to democratic interventions in the legislative process, the following can be stated: As a reaction to the decision of the Federal Constitutional Court, the Bavarian Green party presented a bill in November 2008 which aimed at changing Bavarian police law by prohibiting the use of ANPR without a specific reason. The bill was introduced to the Bavarian Parliament in November 2008 and passed on to the Committee of Interior and

[212] Braun, Frank, "Verfassungsmäßigkeit der Kfz-Kennzeichenerfassung in Bayern", *Bayerische Verwaltungsblätter*, Vol. 142, No. 18, 2011, pp. 549-555.
[213] Bayerischen Staatsministeriums des Innern, "Antwort des bayerischen Staatsministeriums des Innern auf die schriftliche Anfrage des Abgeordneten Florian Ritter SPD vom 01.06.2007 Kennzeichenerkennungssysteme nach Polizeiaufgabengesetz Art. 33", Drucksache 15/8651, Bayerischer Landtag, München, 2013.

Municipal Affairs for further negotiation. In the committee, the governing parties (CSU and FDP) expressed the view that a revision of the law was unnecessary, as it did not interfere with the requirements formulated by the Constitutional Court. The bill was defeated and the law remained unchanged.

Brandenburg

Brandenburg has used ANPR since 2007, when they bought their first three devices. Since then, the number of devices has slowly increased as has the number of deployments. In 2009, ANPR was used in for crime prevention[214] in 37 cases[215], in 2010 in 62 cases[216] and in 2011 in 102 cases[217].

Compared to the other 15 *Länder*, Brandenburg follows a strategy which is, comparatively, significantly focussed on transparency. Since 2008, the Ministry of the Interior reports to the Committee of Home Affairs of Brandenburg yearly about preventive police actions that have made use of ANPR. These reports are public and can be found in the parliamentary documentation. The aim of these reports is to strengthen parliamentary control, and to offer a basis for decisions about extensions of specific provisions of the police law.[218] They contain information about the implementation of ANPR in the previous year, including occasions, number and dates of deployments, and number of hits.

[214] Those reports only offer information about the use of ANPR for crime prevention, they do not tell anything about the use for law enforcement.
[215] Brandenburgisches Ministerium des Innern, "Dritter Bericht des Ministers des Innern an den Ausschuss für Inneres des Landtages über bestimmte Maßnahmen der Datenerhebung auf Grund des Brandenburgischen Polizeigesetzes", Potsdam, 2010.
[216] Brandenburgisches Ministerium des Innern, "Vierter Bericht des Ministers des Innern an den Ausschuss für Inneres des Landtages über bestimmte Maßnahmen der Datenerhebung auf Grund des Brandenburgischen Polizeigesetzes", Potsdam, 2011.
[217] Brandenburgisches Ministerium des Innern, "Fünfter Bericht des Ministers des Innern an den Ausschuss für Inneres des Landtages über bestimmte Maßnahmen der Datenerhebung auf Grund des Brandenburgischen Polizeigesetzes", 2012.
[218] Ibid.

As the Constitutional Court approved the law in Brandenburg, there was no need for an instant revision in 2008. However, a renewal was due in 2010 as the law was limited until 2011. The governing parties in Brandenburg (SPD and DIE LINKE) proposed to make the law permanent. This proposal was discussed in the Committee of Home Affairs and a hearing was conducted in order to assess whether the continuation of the measures was justifiable. Included in the discussion process were several expert hearings. For example, an evaluation of the use of ANPR was commissioned – and eventually carried out by the Max Planck Institute of Foreign and International Criminal Law.[219] In their study, the researchers positively highlighted the actual ANPR practice in Brandenburg. Nevertheless they recommended legal adjustments, especially in relation to the deletion of recorded data. Although not all recommendations were implemented, the results of the study were discussed in parliament and taken into account in the legislative process.

1.4 USING ANPR FOR TOLL CONTROL

Besides the usage of ANPR in the context of police work, it is also deployed in the area of toll control. In Germany, since 2005, all trucks over 12 tons are obliged to pay a road toll – the size of which depends on the street and the distance driven. A private company, Toll Collect GmbH[220], has been assigned to organise the charging and control of the trucks. To achieve this, Toll Collect introduced a satellite based toll system that is based on special devices, so called On-Board-Units (OBU), which are installed in the trucks. From time to time, the OBU transmits data containing information about the streets that have been used. Toll Collect receives the information and charges the trucks accordingly.

[219] Kilchling and Kenzel, 2011.
[220] Partners of the limited liability company Toll Collect are Deutsche Telekom, Daimler and Cofiroute.

1.4.1 The system

In order to prohibit toll cheating, ANPR comes into play in the control system. 300 toll gantries equipped with cameras automatically assess whether the street charge has been paid. To do this, a random sample of 10 per cent of the trucks is checked. The system works as follows:

The gantries take two pictures of each vehicle which approaches the gantry, irrespective of whether the vehicle is obliged to pay or not. One picture comprises the number plate, the other one the vehicle as a whole. With the help of laser devices installed at the gantries, where and when the vehicle passes the gantry, and the size of the vehicle, is recorded. Hence, it can be is checked whether the vehicle possesses the attributes that oblige it to pay a toll.

If no toll is required, the data is deleted immediately. If the system identifies a vehicle that is obliged to pay the toll, whether the vehicle has already paid the toll is checked. To achieve this, two possibilities exist: if the truck possesses an OBU, the gantry tries to establish a connection to the OBU via infrared link in order to receive further information about the truck (number of axles, emission class, weight and number plate). That information is matched with the pictures taken and the results of the laser scan in order to check if the correct amount of money has been paid. If no infrared signal can be received, the truck either has no OBU, and is therefore logged into the system manually, or hasn't paid the toll charge.[221]

To check if the truck has logged in manually, the number plate is extracted from the picture and, together with the information about time and place, this data is matched with the data

[221] Gasch, 2012.

stored in the payment system. If the manual check leads to the conclusion that the truck hasn't paid, the data is sent to the Federal Office for Goods Transport (*Bundesamt für Güterverkehr*) and the relevant procedures are initiated.

1.4.2 Regulation of ANPR for toll control

The legal basis of the toll system in Germany can be found in the BFStrMG (*Bundesfernstraßenmautgesetz*), which defines what kind of vehicles are obliged to pay on which streets. Furthermore it regulates how the toll is collected and the quality assurance systems required to ensure that tolls are paid correctly.[222]

According to the BFStrMG, two types of data are allowed to be collected during the procedure of the collection of the toll: one is related to the route a truck is taking, the so-called *Fahrtdaten*. It includes the street charge that has been paid, the distance the truck has been paid for, the place and time of toll payment and the number plate. In addition, the toll relevant attributes of the truck are collected[223], i.e. the amount of axles, emission class and weight. The operating company, Toll Collect, deletes the route related data after 120 days, and the Federal Office for Goods Transport stores the data for six years. The number plate has to be deleted after three years.

A second type of collected data is the control data (*Kontrolldaten*). It includes a picture of the vehicle, the name of the person driving the vehicle, place and time, number plate and the toll relevant characteristics of the vehicle that is charged. Control data is only allowed to be used for the monitoring of compliance with the rules of the BFStrMG.[224] It is prohibited to transmit or use this data. Rather, it has to be deleted immediately after it has been ascertained that

[222] Ibid.
[223] §4 Abs.3 BFStrMG.
[224] §7 Abs. 2 BFStrMG.

the vehicle is not obliged to pay the street charge or that the toll charge has already been paid. If the toll hasn't been paid, a charging process has to be initiated and Toll Collect has to delete the data as soon as the charging process has been completed. The Federal Office for Goods Transport stores the data for two years.[225]

Both types of data are by law not allowed to be used for crime prevention or law enforcement.[226] The processing of data is strictly bound to the specific purpose of toll collection and control. Nevertheless, as will be shown in section 1.6.2 a loosening of the purpose limitation is regularly called for.

1.5 MEDIA ANALYSIS

1.5.1 Methodology

In order to analyse how, where and when ANPR popped up in the German news, we decided to conduct a media content analysis. Pragmatic has demanded that our content analysis is based on the German press. In order to get access to the relevant articles, we conducted a search in the LexisNexis database, which covers major German newspapers and magazines as well as regional newspapers. The keywords used were:

> *Kennzeichenfahndung, Kennzeichenerkennung, Kennzeichenerfassung, Kennzeichenscanning, ANPR, automatic number plate recognition, Automatisches Kennzeichenlesesystem, Nummernschilderfassung, Nummernschilderkennung, Nummernschildfahndung, Kennzeichen-Scan, Kennzeichen-Überwachung, kfz-*

[225] Gasch, 2012.
[226] Ibid.

Massenabgleich, Kennzeichen-Erfassung, Kennzeichen-Scanning, Kennzeichen-Erkennung, Mautdaten, Maut-Daten, Mautfahndung.

As the first tests of ANPR for crime prevention and law enforcement were conducted in 2002/3, and the German toll system was launched on 31 August 2003, we chose a sample of articles from the past ten years (1 January 2003 to 26 June 2013). The search yielded 1231 articles. We reduced these to a core set based on the following criteria:

1) Less than 500 words. This ensured the elimination of press agency articles, which tend to be capitulatory and thus of relatively poor information content.
2) Thematic restriction (I). The articles had to discuss ANPR at least in a marginal way. The sole mentioning of the term was not sufficient for entering the article pool.
3) Thematic restriction (II). The articles had to discuss ANPR in conjunction with privacy issues / data protection / surveillance etc. This further restriction was necessary, as the initial mishaps of the German toll system produced unwanted 'noise'. This helped to eliminate irrelevant articles.

This approach reduced the number of relevant articles to 145 most relevant articles. Our aim was to cover the most important aspects of the debate and to identify

a) the main stakeholders and their roles
b) their main arguments and influence on the debate
c) the degree to which the controversy was covered by the media
d) the main events that structure the controversy and its media coverage

We did so by generating a code system, which covered four main thematic issues ANPR used by the police, use of toll data for crime prevention / fight against crime, ANPR in security management and ANPR in traffic management. The latter two issues turned out to be rather insignificant and were thus rejected for further analysis. Furthermore, the code system was designed to identify the major stakeholders' recurrent arguments and their impact on the discussion, as well as the main events that created peaks in media coverage.

1.5.2 Results

The final selection consisted mainly of newspaper articles – web based publications and magazines appeared less often (see Table 3).

Table 3: Overview of types of sources of the media analysis

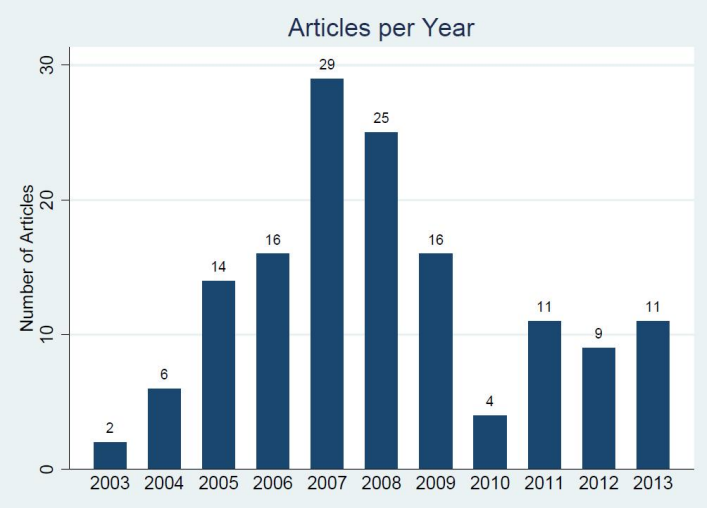
Publication type	**Major (national press)**	**Regional**	**Web based**	**Magazine**
Number of articles	54	53	17	21

Source: Data from LexisNexis Database

The most active newspaper was the national daily newspaper *Sueddeutsche Zeitung* (18 articles) followed by *Frankfurter Rundschau* (11 articles), other national dailies and several regional newspapers (*Der Tagesspiegel*, *Stuttgarter Nachrichten*, each 10 articles) were also of note. Of the web based publications, *Spiegel Online* (5 articles) and *sueddeutsche.de* (4 articles) were the most relevant. From this, it is clear that ANPR is discussed mainly in daily newspapers.

Furthermore, we identified a row of peaks in news coverage that are related to major 'events' connected to ANPR deployment. The most significant event is the decision of the Constitutional Court in 2008, which is covered in most of the articles. Smaller peaks are caused by various criminal cases where truck drivers are involved – the most recent one was the 'truck-sniper', where a truck driver fired haphazardly on other trucks using a variety of small arms weapons between 2008 and 2013. The case was solved in June 2013 by using ANPR, which led to a short news peak. Generally speaking, the number of articles per year decreases sharply after the constitutional court decision in 2008 (see diagram below).

Articles per year



Source: Fraunhofer ISI analysis of LexisNexis database

1.6 KEY STAKEHOLDERS

Various stakeholders with different interests and levels of engagement are directly or indirectly involved in the ANPR surveillance practice. This section aims at giving a structured overview of the stakeholders involved in controversies related to ANPR. We follow a definition of a *stakeholder* that focuses on the idea that any group or individual who can affect, or is affected by, the surveillance technology ANPR is a stakeholder.

For the purpose of analysing stakeholders, the following questions have a guiding function:

- Who are the watched? Whose fundamental rights might be infringed by the use of ANPR?
- Who are the watchers?
- Who establishes the conditions for the use of ANPR?
- Who watches the watchers?

As follows, the relevant stakeholders for both application areas are illustrated.

1.6.1 ANPR used by the police

Citizens

Those who are watched are in very general terms the citizens. To be more specific, people who drive a car on streets where ANPR is used are in the centre of this surveillance practice. It can be assumed that a majority of the population does not even know that ANPR exists in Germany. Although the media analysis reveals that it is a subject of discussion in the German press, there is no broad on-going public debate.

Since there is no other data available, one (admittedly limited) approach to solidify the car driver as a stakeholder is to consider those who handed in constitutional complaints as representatives of individual car drivers and analyse their position and lines of argumentation. In his role as a citizen, for instance, the plaintiff who handed in a complaint against ANPR in Bavaria[227] argued that it is not proportional to scan every car. The main point of criticism is the interference with the right on informational self-determination. In addition, it is argued that the high error rate leads to disproportional control situations. Furthermore, he claims that this general suspicion has a deterrent effect on society. The arguments that were brought forward by the other plaintiffs in Lower Saxony, Baden-

[227] The case: Benjamin Erhart commutes regularly on highways in Bavaria. He handed in a complaint and argued that ANPR is disproportional since a lot of incorrect hits occur. The Administrative Court in Munich decided that ANPR in Bavaria is constitutional because the data is deleted immediately. Therefore the Court dismissed the action. Erhart decided to appeal on points of law and wants to bring the case to the Federal Administrative Court. Further information and documents can be found online on the website of the plaintiff: http://benjaminerhart.com/kennzeichenscanning/.

Württemberg and Hesse are similar. Due to a lack of surveys, there is little alternative approach to capture public perception directly.

The police forces

The police forces are those who watch. Again, the media analysis has shown that the police forces of the *Länder* mostly support ANPR. It is argued, and hoped, that ANPR will increase security. The conditions for the use of ANPR are (partly) established in the police laws of the different *Länder*. Therefore parliamentary discussions and political majorities decide on the introduction, adjustment, prolongation or abolition of legal provisions for ANPR. For instance, the liberal-conservative party strongly emphasises the importance of ANPR and states that it increases security and that it is proportional. They emphasise the benefits of ANPR concerning crime prevention, while the interference with basic rights is regarded as marginal, as the data is deleted in case of a non-hit.

Data Protection Commissioners

The 16 independent Data Protection Commissioners of the *Länder,* and the Federal Commissioner for Data Protection, have an advisory, but not a legally binding function on the state parliaments and the German *Bundestag*. Almost all of them have been following the discussions about ANPR in their respective *Land* and have mostly positioned themselves rather critically. They monitored the developments in relation to the amendments to respective legislative acts before and after the Constitutional Court decision and expressed their doubts about the constitutionality and proportionality in their annual reports as well as in their exchanges with the Ministries of the Interior. A further main point that was brought into the discussion by the Data Protection Commissioners is potential function creep, meaning that purpose limitation might be eroded after a while. For instance, they point to the possibility that the generation of movement profiles of cars and car drivers might be perceived as a necessity in the future.

Drivers' Associations

Further influential voices that do not fall under a narrow definition of a stakeholder can be identified. For instance, the German drivers' association (ADAC) is an influential actor who shapes the public debate. The ADAC as an actor itself emerges rather often as soon as ANPR (or any other car or transportation relevant issues) becomes a topic of political discussion. They position themselves strongly against ANPR by arguing that the use of the technology is not proportionate and that success rates are low. In addition, they frame ANPR as unnecessary total surveillance and emphasise its unconstitutionality. In 2008, a legal assessment commissioned by the ADAC was conducted. This report came to the conclusion that most of the provisions in the *Länder* were unconstitutional.[228] This report was heavily cited and supported critical public voices before and after the decision of the Constitutional Court.

Controversy: Constitutional Complaint and Court Decision in 2008

One event that heavily shaped the use of ANPR in Germany is the 2008 ANPR decision of the Federal Constitutional Court. Initial discussions about legal issues were initiated in Hesse, when a new police law was introduced in the beginning of 2005 that allowed the police to use ANPR without a specific reason and without restriction to a specific street. Following this, the Constitutional Court in Hesse received a complaint against ANPR in 2005.[229] In his statement the plaintiff referred to the 2006 decision of the Federal Constitutional Court on dragnet investigations, in which the Court had ruled that dragnet investigations are only allowed if a concrete danger exists – a general situation of increased threat is not sufficient for an encroachment on the fundamental right to informational self-determination.[230]At the same time, a constitutional complaint against the provisions in Schleswig-Holstein was handed in as well.

[228] Roßnagel, *Kennzeichenscanning - Verfassungsrechtliche Bewertung*, 2008.
[229] Staatsgerichtshof des Landes Hessen, "Grundrechtsklage - P.St. 2047 - ", Press Release, 20 September 2005.
[230] BVerfGE 115; 320.

Since 2007, the Federal Constitutional Court had been dealing with these cases and decided in 2008 that the challenged provisions in Hesse and Schleswig-Holstein were unconstitutional:

> "The provisions do not comply with the precept of determinedness and clarity of legal provisions because they neither determine the cause nor the purpose of investigation which both the recognition and the matching of the data are intended to serve. Over and above this, the challenged provisions, in their undefined scope, also do not comply with the constitutional precept of proportionality. They make severe interference with the affected parties' right to informational self-determination possible without sufficiently codifying the statutory thresholds which fundamental rights demand for measures that constitute such intense interference." [231]

The Court argued that the fundamental right to informational self-determination is infringed, if the number plates "are not promptly matched against the tracing files and deleted without further evaluation". Furthermore, the challenged provisions did not fulfil the requirement that "interference with the fundamental right to informational self-determination must have a statutory basis that is constitutional"[232].

As a reaction to the Court decision, Schleswig-Holstein voided its regulation and Hesse revised its police law. In addition, as described above, some *Länder* have changed their legal provisions since then.

[231] BVerfGE 120; 378
[232] BVerfGE 120; 378.

Obviously, as the reaction of the *Länder* shows, the Federal Constitutional Court set a milestone and forced the *Länder* to revise their law if they wanted to implement ANPR. The Court fulfilled its function to protect the fundamental rights of the citizens. The requirement that the provisions clearly have to define the conditions under which it is permissible to use ANPR benefits the individual citizen insofar as he knows what measure he has to accept when.

1.6.2 ANPR used for toll control

The media analysis reveals that similar stakeholders to the above play key roles in discussions about the use of the ANPR in toll collection. As already mentioned, the toll gantries and related data are, by law, only allowed to be used for toll control. Nevertheless, politicians – mainly from the conservative party – regularly call for the use of the toll system to trace criminals. Again, it is argued that it is necessary for effective police work and that this would lead to an increase in security. Another line of argumentation directly focuses on the persons affected: some politicians hold the view that it is irresponsible not to use the available data, and difficult to justify why the data is not used. They argue that in the case of non-use, the perpetrator is protected instead of the victim. In the course of the introduction of a number of counter-terrorism laws in 2007 ("*Schäuble-Katalog*") the federal ministry of the interior argued that the toll gantries should be used for crime prevention and law enforcement. Minister Schäuble stated that the importance of effective law enforcement outweighs that of data protection in the case of serious crime and terrorism. The Federal police also welcome a suspension of the purpose limitation principle. They say law enforcement would be facilitated and if the use is only limited, the danger of total surveillance does not exist.

Contrary to this, the Data Protection Commissioners for the *Länder* position themselves against the use of toll data for law enforcement. Their line of argumentation focuses on the high error rate of the system, the disproportionality of the measure and the danger of total surveillance. Even if the use is at first restricted to serious crimes, it might easily be

expanded to other kinds of crime. Further, it might be difficult to argue why only truck drivers should be surveilled and not every vehicle. In addition, they do not see a necessity for this tool to be used by the police.

Controversy: Using the toll system for law enforcement

Ever since the truck toll was introduced in Germany, discussions have taken place about the use of the recorded data for purposes other than those originally foreseen. In 2004, when the legal basis for the toll system was negotiated, the German Parliament discussed the possible use of toll data for law enforcement purposes, but finally the Bundestag adopted a law with strict purpose limitation. Hence, a legislative amendment would be necessary to use the toll data for law enforcement.

The truck drivers' and logistics companies' lobby did not explicitly focus on surveillance issues. Instead, it was the additional costs that were see as a financial burden. Also, the Federal Commissioner for Data Protection and Freedom of Information and also some data protection commissioners of the *Länder* criticised the lack of transparency in the negotiations between the Federal Ministry of Transport, Building and Urban Development and the corporations responsible for the implementation of the scanning system.

Although it has, until now, not been legally permitted, the gantries have the potential to be used as a large scale surveillance tool and accordingly, debates about the use of the system for criminal investigations regularly re-emerge.[233] Nevertheless, due to a lack of political intent, such ideas have never been enacted.

[233] Just recently, in November 2013, a working group of the conservative party preparing the coalition negotiations after the parliamentary elections demand loosen the purpose restriction. See Diehl, Jörg, Frank Dohmen, Veit Medick, et al., "Überwachung: Innenminister Friedrich greift nach Maut-Daten", *Spiegel Online*, 06 November 2013.

1.7 HOW THE ORGANIZATION HAS ENGAGED WITH THE PUBLIC AROUND ITS USE OF THE SURVEILLANCE PRACTICE

Concerning ANPR for crime prevention and law enforcement, the police and the Ministries of the Interior of the *Länder* are rather uncommunicative in terms of engagement with the public. In fact, car drivers do not often know when and where number plates are scanned. Following a common line of argumentation, the increase of security through the use of ANPR is more important than the democratisation of the system. This position became quite obvious in June 2013, when the Federal Police released that they have been using ANPR for a couple of months to find a suspect. This was only made public only after they found the suspect with the help of ANPR. Obviously, the police see it as an advantage, if the locations of the ANPR devices are not known. Hence, engagement with the public happens only occasionally, and in a reactive manner, or when the authorities claim the use as a success.

Therefore, it has to be concluded that real engagement with the public does not exist, not even in an informational manner. Press releases occur occasionally, but there is no consistent or identifiable media strategy which aims at explaining, informing or engaging the public. The places where discussions about the pros and cons of this surveillance technology occur are in policy arenas. Representatives of different pressure groups and scientific experts are given a say in policy-making processes – at least formally. In principle, it is possible to trace those political discussions through publicly available parliamentary documentation. In practice, however, this is only done by a very small fraction of society. Those who actually engage themselves show a special interest in surveillance and data protection related topics.

1.8 HOW MEMBERS OF THE PUBLIC HAVE ENGAGED WITH THE ORGANISATIONS WHO USE THE SURVEILLANCE PRACTICE

In general, a prerequisite for an interaction with the organisations that deploy and use surveillance technologies is that people know that such technologies exist, that they are in use, what they are used for, how they work and how they are regulated. Due to the fact that there is no general public debate about ANPR in Germany (one result of the media analysis is that it appears that media interest was high only shortly before and after the Constitutional Court decision), it can at least be questioned whether there is a critical mass of people who know about ANPR and the use of ANPR by the police. The variety of regulations and practices increases the complexity and further contributes to this situation. Public debates only appear as soon as the purpose limitation of the toll gantries is questioned. Then, the surveillance potential of the toll infrastructure becomes a matter of interest.

In terms of public engagement with the organisations that use this surveillance practice, the following observation can be made:

First, the claims that have been handed in against ANPR were a momentous way of engaging with the surveillance practice and the authorities deploying ANPR. The fact that the Federal Constitutional Court – as the highest judicial authority –dealt with ANPR in two *Länder* reflected an important step in the history of ANPR. The Court decision forced the *Länder* to clearly define the requirements under which ANPR is allowed, and therefore supported citizens in their fundamental rights. For instance, by regulating the retention dates and requiring an immediate deletion of the collected data, the Court made a strong case for the citizens. Nevertheless, as a matter of fact, there is also the other side of the coin: In practice, the 16 *Länder* handle the Court decision differently which makes the deployment questionable in terms of constitutionality. This becomes obvious by the fact that currently claims against provisions in four *Länder* are pending. In addition, those who handed in

complaints are not satisfied with the decision, since they regard the scanning and analysis of the number plate, in itself, as a violation of basic rights.

Second, engagement activities can mostly be detected within a small group of activists, who are particularly interested in surveillance and data protection issues. But there is no engagement on a large scale, which is indeed related to the lack of transparency. This assumption is based on two observations: First, those who handed in constitutional complaints fall in this group. For instance, the person who applied to the Court because of ANPR use in Bavaria, is active in the German Working Group on Data Retention[234] and works closely together with members of the Pirate Party[235]. Second, a blog that critically analyses developments within the digital society (netzpolitik.org) published the – until then publicly unknown – locations of the fixed ANPR devices in Brandenburg. Certainly, the police see this as a threat to their everyday work, since criminals might just use different routes if they know where the devices are located.

1.9 CONCLUSION

In the first instance, it can be stated that ANPR is *de facto* not used as a nationwide, large-scale, surveillance tool. Rather, the situation differs vastly between different regions in Germany; some *Länder* do not possess any devices at all, some only a few – only Bavaria owns more than 20. All in all, around 70 ANPR devices used for policing exist in Germany. Moreover, the frequency of use differs between the *Länder*. While one *Land* uses ANPR permanently, others deploy it only seldom. Compared to other countries such as the United Kingdom, the deployment of ANPR systems for policing is almost negligible.

[234] Salch, Andreas, " Die Polizei, dein großer Bruder", *Süddeutsche.de*, 19 October 2011. "Arbeitskreis Vorratsdatenspeicherung", see http://www.vorratsdatenspeicherung.de/
[235] See e.g. http://www.daten-speicherung.de/

The 300 toll gantries installed nationwide for compliance checking and enforcement do indeed have the potential to function as a large surveillance tool. Currently, the use of the gantries is strictly bound to the specific purpose of toll control and their use is restricted to random checks. Therefore the collected data is deleted immediately in case of a non-hit. Nevertheless, discussions and political demands aiming at relax the purpose limitation regularly occur. This clearly shows there is a certain will behind the relaxation of purpose limitation.

What stands out in the German case is the strong top-down control of ANPR: A look at the legal situation in Germany reveals that the Federal Constitutional Court clearly defined restrictive prerequisites for the use of ANPR by the police. Interestingly enough, as the reaction of the *Länder* shows, there is obviously room for interpretation about how exactly the Court decision feeds into the police laws of the *Länder*. As a matter of fact, the *Länder* reacted differently to the Court decision. This is reflected in the variations in current regulations and practices. These different developments are highly contested – which is reflected by the pending claims against ANPR provisions in different *Länder*. Hence, controversies surrounding ANPR are obviously not resolved. There is still a high degree of uncertainty about the constitutionality of ANPR use that leads to very reluctant behaviour on the part of the main actors.

Citizens' resilience towards ANPR is rather limited. The majority of people are either not interested in ANPR practices, or does not know that the police use ANPR. Due to a rather reactive approach to public communication, the possibilities to be resilient are restricted. As a result of this lack of transparency, there is no engagement on a large scale – only a small group of activists publicly oppose ANPR use by the police. Based on the rather critical reactions to discussions about the loosening of the strict purpose limitation related to toll data, it can be assumed that; if people knew about the usage of ANPR by the police, a

majority would oppose such use. Another actor who influenced the public debate about ANPR after the Court decision in 2008 is the German drivers' association – ADAC – which positions itself against ANPR. ADAC commissioned and published a study which strongly criticises ANPR.

To conclude, it can be stated that technically, the infrastructure in Germany would allow ANPR to be used as a large-scale surveillance tool. However, in practice, it is prohibited by law to use the toll gantries for any purpose other than toll control. In fact only 10 per cent of the gantries are in use at any given time. Although attempts have been made to abolish strict purpose limitation, there was never enough political support for such an initiative. Although public debates about the toll infrastructure and its surveillance capacity took place, the issues raised by mobile and fixed ANPR devices used by the police elicited virtually no public interest. The extent and scope of ANPR use differs between the Länder and is not comparable with the toll infrastructure. Nevertheless, the interest in ANPR obviously exists, and taking into account that some *Länder* introduced ANPR through certain 'back-door' procedures, possible future scenarios cannot exclude the use of the gantries for other purposes than originally foreseen.

Literature

Arzt, Clemens, "Rechtsfragen der automatisierten Kennzeichenerkennung", *Straßenverkehrsrecht*, Vol. 4, No. 9-10, 2004, pp. 368-373, 368-373.

"Autobahn-Schütze handelte aus "Frust"", Tagesschau.de, 25 June 2013. http://www.tagesschau.de/inland/autotransporter102.html

Bayerischen Staatsministeriums des Innern, "Antwort des bayerischen Staatsministeriums des Innern auf die schriftliche Anfrage des Abgeordneten Florian Ritter SPD vom 01.06.2007 Kennzeichenerkennungssysteme nach Polizeiaufgabengesetz Art. 33", Drucksache 15/8651, Bayerischer Landtag, München, 2013.

Brandenburgisches Ministerium des Innern, "Dritter Bericht des Ministers des Innern an den Ausschuss für Inneres des Landtages über bestimmte Maßnahmen der Datenerhebung auf Grund des Brandenburgischen Polizeigesetzes", Potsdam, 2010.

Brandenburgisches Ministerium des Innern, "Vierter Bericht des Ministers des Innern an den Ausschuss für Inneres des Landtages über bestimmte Maßnahmen der Datenerhebung auf Grund des Brandenburgischen Polizeigesetzes", Potsdam, 2011.

Brandenburgisches Ministerium des Innern, "Fünfter Bericht des Ministers des Innern an den Ausschuss für Inneres des Landtages über bestimmte Maßnahmen der Datenerhebung auf Grund des Brandenburgischen Polizeigesetzes", Potsdam, 2012.

Braun, Frank, "Verfassungsmäßigkeit der Kfz-Kennzeichenerfassung in Bayern", *Bayerische Verwaltungsblätter*, Vol. 142, No. 18, 2011, pp. 549-555.

Bundeskriminalamt, "Bundesweite Serie von Schüssen auf Autotransporter: Pressekonferenz anlässlich der Festnahme eines Tatverdächtigen", Press Release, 25 June 2013. http://www.bka.de/nn_233148/DE/Presse/Pressemitteilungen/Presse2013/130625__BAOTransporterPressekonferenz.html

Diehl, Jörg, Frank Dohmen, Veit Medick, and Fidelius Schmid, "Überwachung: Innenminister Friedrich greift nach Maut-Daten", *Spiegel Online*, 06 November 2013. http://www.spiegel.de/politik/deutschland/ueberwachung-innenminister-friedrich-fordert-zugriff-auf-maut-daten-a-931952.html

Gasch, Patrick, *Grenzen der Verwertbarkeit von Daten der elektronischen Mauterfassung zu präventiven und repressiven Zwecken*, Duncker & Humblot, Berlin, 2012.

Guckelberger, Annette, "Zukunftsfähigkeit landesrechtlicher Kennzeichenabgleichsnormen", *Neue Zeitschrift für Verwaltungsrecht*, Vol. 28, No. 6, 2009, pp. 352-358.

Hessischer Minister des Inneren und für den Sport, "Antwort des hessischen Ministers des Innern und für Sport auf die kleine Anfrage des Abg. Jürgen Frömmrich (BÜNDNIS 90/DIE GRÜNEN) betreffend Einsatz von Kennzeichenlesegeräten in Hessen", Drucksache 18/7590, Hessischer Landtag, Wiesbaden, 2013.

Kenzel, Brigitte, *Die automatische Kennzeichenfahndung. Eine neue Überwachungsmaßnahme an der Schnittstelle zwischen präventivem und repressivem Einsatz*, Verlag Dr. Kovaĉ, Hamburg, 2013.

Kilchling, Michael, and Brigitte Kenzel, "Recht und Praxis der anlassbezogenen automatischen Kennzeichenfahndung, Verkehrsdatenabfrage und Mobilfunkortung zur Gefahrenabwehr in Brandenburg. Wissenschaftliche Begleitforschung zu den §§ 33b Abs.3, Abs. 6 Satz 2 und 36a BpgPolG", Gutachten, Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2011.

Landesbeauftragten für den Datenschutz Rheinland-Pfalz, "Offene Datenschutzfragen im Ermittlungsverfahren gegen den Autobahnschützen", Press Release, 25 June 2013. http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2013062501.

Landesregierung Niedersachsen, "Antwort der Landesriegierung auf die Kleine Anfrage der Abgeordneten Johanne Modder, Klaus-Peter Bachmann, Heiner Bartling, Karl-Heinz Hausmann, Jürgen Krogmann, Sigrid Leuschner, Jutta Rübke und Ulrich Watermann (SPD)", Drucksache 16/2386 neu, Niedersächsischer Landtag, Hannover, 2010.

Landesregierung Schleswig-Holstein, "Automatisierte Kennzeichenerfassung nichtig – Innenminister Lothar Hay: Urteil ist Mahnung und Auftrag zugleich", Press Release, 11 March 2008. http://www.schleswig-holstein.de/ArchivSH/PI/IM/2008/080311_im_kfzScanning.html.

Martinez Soria, José, "Grenzen vorbeugender Kriminalitätsbekämpfung im Polizeirecht: Die automatisierte Kfz-Kennzeichenerkennung", *Die Öffentliche Verwaltung* 18/2007, pp. 779-785.

Roßnagel, Alexander, *Kennzeichenscanning - Verfassungsrechtliche Bewertung*, ADAC e.V., München, 2008.

Roßnagel, Alexander, *Kennzeichenscanning – Umsetzung der Vorgaben des Bundesverfassungsgerichtes*, ADAC e.V., München, 2009.

Salch, Andreas, " Die Polizei, dein großer Bruder ", *Süddeutsche.de*, 19 October 2011. http://www.sueddeutsche.de/bayern/klage-gegen-kennzeichen-erfassung-die-polizei-dein-grosser-bruder-1.1168319

Staatsgerichtshof des Landes Hessen, "Grundrechtsklage - P.St. 2047 - ", Press Release, 20 September 2005. http://www.staatsgerichtshof.hessen.de/irj/Staatsgerichtshof_Internet?rid=HMdJ_15/Staatsgerichtshof_Internet/nav/607/6071021f-824b-c11a-eb6d-f197ccf4e69f,05e10d1c-5d71-ec11-f3ef-ef97ccf4e69f,,,11111111-2222-3333-4444-100000005002%26_ic_seluCon=05e10d1c-5d71-ec11-f3ef-ef97ccf4e69f%26shownav=false.htm&uid=6071021f-824b-c11a-eb6d-f197ccf4e69f&shownav=false.

German Federal Constitutional Court Cases

BVerfGE 65; 1: Population Census, 15.12.1983 (BVerfG 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83 and 1 BvR 484/83)

BVerfGE 120; 378: Automatic license plate comparisons, 11.03.2008 (BVerfG 1 BvR 2074/05 and 1 BvR 1254/07)

BVerfGE 115; 320: Dragnet Investigation II. 04.04.2006 (BVerfG 1 BvR 518/02)

BVerfG BvR 1443/08; Constitutional complaint against automatic mass car license plate screening in Baden-Wurttemberg, 30.11.2009

BVerfG BvR 3187/10; Constitutional complaint against automatic mass car license plate screening in Hesse, 21.12.2010

BVerfG BvR 2795/09; Constitutional complaint against automatic mass car license plate screening in Bavaria, 11.08.2011

Legal Documents

BFStrMG, Bundesfernstraßenmautgesetz (Law about toll for federal motorwys) of 12 July 2011 (BGBl. I p. 1378), last changed by article 2 paragraph 152 of the law of 7 August 2013 (BGBl. I p. 3154)

GG, Grundgesetz (Basic Law) for the Federal Republic of Germany of 23 May 1949 (BGBl. I p. 1), last amended by article 1 of the law of 11 July 2012 (BGBl. I p. 1478)

StPO, Strafprozessordnung (code of criminal procedure) of 07 April 1987 (BGBl. I p. 1074), last amended by the law of 24 September 2013 (BGBl. I S. 3671)

IRISS WP3: ANPR Group

Case study report on the Electronic Toll System In Slovakia

Written by Erik Láštic, Comenius

1. Introduction

Automatic Number Plate Recognition (ANPR) technology in Slovakia is deployed, or is to be deployed in several areas. First, it is used as a technology to control vehicle access in buildings and parking lots. The second area of deployment of the ANPR has to do with the launch of two new databases (Central Registry For Offences and National System of Traffic Information, planned for 2015) that will use ANPR data for monitoring and for law enforcement. Third, ANPR technology is going to be found in police cars as a part of a new hardware project that was presented in the 2013 and is to be introduced from 2014. Fourth, ANPR is tested by private companies for use against driving offences on Slovak roads, as a part of legal changes that introduced driver's absolute liability in 2012. Fifth use that is the subject of this case study, as it is the only one fully implemented on the national scale, is the use of ANPR as one of the technologies that are deployed in Electronic Toll System (further as "ETS") launched in 2010.

The report will briefly describe state of the affairs in the second, third and fourth area and then move to a comprehensive review of the Electronic Toll System in Slovakia.

Central Registry For Offences and National System of Traffic Information

Two databases are planned for launch in near future by the government. In both cases, the preparatory document and press reports suggest that databases will be directly

interconnected with ETS information system. In first case, an impact assessment report for the new 2013 law on toll mentions the new Central Registry for Offences that will be established in the near future (2015) for administration of traffic offences. The IAR explicitly acknowledges that the registry will use data gathered by the existing technical infrastructure that is part of ETS information system (e.g. portable and stationary gates, camera systems, radar and laser systems). No other policy details are available on the Central registry. The data from ETS database will also be used in another project, this one coordinated by the Transport Ministry, called *National System of Traffic Information*. The main function of the system is to provide complex monitoring of traffic situation on Slovak roads.[236]

KITT for Slovak Police[237]

"Police cars of the future", "Police to drive intelligent cars", these are only two of many headlines from Slovak media that informed in November 2013 about new cars for Slovak Police that will be used for crime prevention and law enforcement.[238] Approximately 800 police cars (out of 4000) will use new hardware installation with touchscreen, integrated card reader and camera with HDD recording and ANPR capability. The system is interconnected with several police databases (e.g. driver licences, car registrations, stolen vehicles, IDs, operational centre) and will allow police officers real-time control of persons and vehicles. First 400 cars will be employed from 2014. The new cars are part of 40 million EURO project coordinated by the Interior Ministry called *Electronic services of National Database of vehicles*, which is co-financed from EU cohesion funds. [239]

---

[236] The main angle of the article however confronts sudden change in estimated price tag for the project that went from 150 million EURO in 2012 to only 15 million EURO this year. See SME, 10/12/2013, Informácie o zápchach náhle zlacneli (Traffic Information are suddenly cheaper), Available at: http://ekonomika.sme.sk/c/7035358/informacie-o-zapchach-na-ceste-nahle-zlacneli.html, accessed 10/12/2013

[237] See for example, http://automoto.cas.sk/clanok/193285/ukazali-policajne-auta-buducnosti

[238] See for example: SME, Polícia bude jazdiť na inteligentných autách (Police will drive intelligent cars), 20/09/2013, available at: http://auto.sme.sk/c/6941905/policajti-budu-jazdit-na-inteligentnych-autach.html, accessed 09/10/2013

[239] For the description of the project see http://www.minv.sk/?ES_NEV_MV

Driving offences and the ANPR

In 2012 the Slovak parliament amended the traffic law and introduced absolute liability for traffic offenses. As the Interior Ministry argued in its reasoning report, the amendment aimed to decrease the number of fatalities on the roads, to protect disciplined drivers against road pirates and to limit the scope of administrative freedom of police, thus limit corruption. As the Ministry explained in following weeks, the legal change will be complemented by implementation of ANPR technology that will include an intelligent system that would provide administrative infrastructure for automated delivery of fines. The immediate media debate focused almost exclusively on financial aspect of the changes.[240]

Although the law has been effective since July 2012, the ANPR is yet to be implemented. The early parliamentary elections in 2012 postponed the preparation of the public procurement. Also importantly, the ANPR is deployed only in limited scope for traffic analysis and covers only main highways, so the state has to invest massively into ANPR infrastructure to cover relevant roads in Slovakia[241]. This type of investment will need a political support in times of scarcity, but will also be complicated from public procurement point. As early media reports discovered, the pilot testing overwhelmed the police as the test delivered hundreds of hits that proved too much for the police to administer.[242] The media also reported that several private companies were testing their technologies, probably preparing for the public procurement. It has yet to be seen whether the Interior Ministry will look for a complex solution that will include both ANPR infrastructure and an information system that will connect ANPR with database of vehicles and allow for automatic distribution

[240] The debate reemerged three times during 2012. In January, when the law was passed, July, when the law became effective, and September, when the media investigated whether the police actually implemented the law.
[241] See for example: SITA, "Avizované radary na cestách od leta nebudú" (Announced Radars on Roads Delayed Indefinitely), 01/02/2012, , available at http://automoto.cas.sk/clanok/188160/avizovane-radary-na-cestach-od-leta-nebudu, accessed 04/10/2013
[242] See SME, Radary vás zatiaľ samy nechytia (Radars will not catch You), 03/07/2012, available at: http://auto.sme.sk/c/6444840/radary-vas-zatial-samy-nechytia.html, accessed 09/07/2013

of tickets, or they will be split into two processes. So far only online discussions on articles informing about introduction of absolute liability emerged, not surprisingly with negative opinions about the government plans to grab more money from citizens. Only few comments raised questions about constitutionality of ANPR technology in use, citing violations of privacy rights as an example[243]. In 2013 the Ministry of Interior announced that the public procurement would be delayed indefinitely due to budget constraints. In recent interview the Interior Minister R. Kaliňák also raised the possibility that the ANPR system will be introduced as public-private partnership (PPP) project, in the same way as the ETS in 2010.[244]

2. Methodology

The topic of vehicle surveillance has not been investigated in Slovakia at all. Without offering extensive explanations for the lack of research on Slovakia, that has to do with limited pool of researchers, the topic of surveillance is only recently getting media attention due to Snowden case and several policy initiatives that are (in)directly connected to surveillance (e.g. E-health initiative, E-register of citizens).

Throughout the report we provide multiple evidence about the electronic toll system that is regarded predominantly as a financial levy imposed by the state, by both the watchers and watched. The dominant angle that appears is not that of the surveillance, but of the economical impact of the ETS. The system was introduced to increase budget revenues; the operator of the system, a private company that operates system is motivated by the profit. The subjects of the toll, haulier companies and drivers use various techniques to avoid ETS,

[243] See discussion under article SME, Polícia pokuty poštou neposiela (The police does not send fines by mail), 02/09/2012, available at http://www.sme.sk/diskusie/2043116/1/Pokuty-postou-policia-neposiela.html, accessed 09/11/2013. User ///o-o\writes "Citizens have a right to data protection, and ANPR has to work with accordance to law. I doubt that current testing of ANPR technology is legally OK. One of the most fundamental obligations is a visible information that premises are monitored, so that a citizen is aware of possibility of being recorded."

[244] See the 2013 interview with Interior Minister R. Kaliňák, available at: http://automoto.cas.sk/clanok/193268/policajti-vam-automaticky-pokutu-neposlu, accessed 03/12/2013

but their motivations are also financial. Critical events and responses to the ETS are motivated by the costs, not the privacy. Because of this, the aspect of personal data and the privacy is missing altogether from legal, political and public discussions about the ETS. The same is true for ETS as a form of surveillance. While this "lack of surveillance aspect" is understandable to a large extent, in case of the ETS in Slovakia it is more profound due to lack of activity of stakeholders (Slovak DPA, NGO's, Courts) that have capacity to shift attention to other aspects of the ETS than financial. This lack of advocacy in data protection and surveillance is by no means limited only to ETS, but is the natural state of things in Slovakia so far.

However, as we will show, the lack of debate and the invisibility of the surveillance aspect of the ETS do not mean its nonexistence. They do appear in a form of a creeping legal extension of the access to ETS data by various state agencies (Police, Secret Service), but also by current plans to use the ETS data for other purposes than tolling. With this in mind, our study is based on extensive desk research that includes variety of primary sources, e.g. legislation, consultation documents, legal contracts, parliamentary transcripts and reports and secondary sources, e.g.: media articles. For media analysis we used a comprehensive media database that offers transcripts for TV, radio and print content. We also searched the Internet for various topics in connection to ETS and surveillance in order to find Internet discussions, forums and social groups[245]. Some additional information was gathered via

[245] E.g. Facebook group, Podporujem dopravcov v štrajku (I Support Haulers in Their Strike) that has 57 000 members and is active since introduction of ETS in 2010. Available at https://www.facebook.com/pages/Podporujem-dopravcov-v-štrajku-Mýto-sa-týka-nás-všetkých/226312988873, accessed 09/11/2013

email exchanges[246] with stakeholders, especially when attempting to fill gaps about surveillance side of ETS and its implementation.[247]

3. Key stakeholders in the ETS

For the identification of key stakeholders we used three sources. First, we looked at the consultation phase in the legislative process at the governmental level, in which anyone is allowed to comment on proposed legislation. Second, we analyzed 2007 and 2013 laws on electronic toll and looked for subjects explicitly mentioned in texts. Finally, we analyzed extensive media monitoring of TV, radio and printed media between 2005 and 2013 and filled missing stakeholders. While not included in the list of stakeholders, the media played a important role in informing public about the procurement, launch and the implementation of the ETS in Slovakia, including major controversies, e.g.: public procurement and winning bid by SkyToll, unknown ownership of the SkyToll, protests surrounding the launch of the ETS, strategies of avoiding the ETS.

Following is the list of key stakeholders with their brief description.

- **Ministry of Transport, Construction and Regional Development of Slovakia** legal, political and policy stakeholder, drafted and submitted all relevant ETS legislation, supervises National Highway Company
- **Národná diaľničná spoločnosť** (National Highway Company, JSC, fully owned by the state), ETS administrator, accountable to the Ministry of Transport, in charge of the management and maintenance of the highways and motorways in Slovakia

[246] We used this source in order to fill gaps after desk and media research. We asked representatives of Skytoll, Police of Slovak Republic and Slovak Data Protection Agency questions that were related to data protection and use of ETS forthe law enforcement. The emails to Police went unanswered, the email to SkyToll and Slovak DPA either provided only general information or refused comment.
[247] Because Slovakia is a small unitary state, the preparation and implementation of the national ETS was not confronted with issues connected to federalism as in Germany or Belgium.

- **SkyToll, a.s**. (SkyToll, JSC)[248], the operator of the ETS. A private company owned fully by Ibertax, a.s. [249] , Responsible for the delivery and operation of the ETS based on the contract [250] on the Provision of Comprehensive Service of Electronic Toll Collection entered into by NDS (852 millions EURO[251]); used and uses various subcontractors for different aspects of the ETS, e.g. payment services[252], FleetPay (JSC)[253], or Q-Free[254], subcontracted for central tolling and enforcement system
- **Toll Police Force,** established by the law as a separate unit within the Police Force of Slovakia, responsible for legal enforcement of the ETS
- **Haulers Interest Groups**
    - *Associations of Road Transport Operators of the Slovak Republic* (ČESMAD), www.cesmad.sk , biggest interest group of haulers, also subcontracted by the SkyToll for operating "contact points[255] that provide various services, e.g. authorized installing of OBUs[256]
    - *Union of Motor Carriers* (UNAS), www.uniadopravcov.sk, interest group launched in 2009 in response to the ETS, more radical than CESMAD, was behind blockade of the main roads in January 2010, operated an Facebook group (I Support Strike of Haulers, E-Toll is Everyone's Problem) with over 50 000 members[257]

[248] See Business Registry entry, http://www.orsr.sk/vypis.asp?ID=141278&SID=2&P=0&lan=en
[249] The Ibertax, a.s. company does not list its owners and uses shares on the name which can be transfered freely, (11 in total), See http://www.orsr.sk/vypis.asp?ID=88330&SID=2&P=0&lan=en
[250] The Toll contract between NDS and SkyToll is available here (in Slovak), http://www.scribd.com/doc/13110068/Zmluva-NDS-a-SkyToll, Accessed 09/11/2013
[251] See, http://datanest.fair-play.sk/datasets/2/records/37156
[252] See SME, Ku SkyTollu prišla ďalšia firma, ktorá zarobí na mýte (Another Company Joins SkyToll to Earn Money), 16/04/2010, available at: http://ekonomika.sme.sk/c/5330656/ku-skytollu-prisla-dalsia-firma-ktora-zarobi-na-myte.html?utm_source=link&utm_medium=rss&utm_campaign=rss, accessed 09/11/2013
[253] See Business Registry entry, http://www.orsr.sk/vypis.asp?lan=en&ID=161109&SID=2&P=0, accessed 09/11/2013
[254] See, Factsheet by Q-Free, http://q-free.pingbull23.com/files/2012/11/TruckTollingSlovakia.pdf, accessed 07/12/2013
[255] See the scale of the services provided by the contact points, available at: https://www.emyto.sk/web/guest/contact-points, accessed 07/12/2013
[256] See, http://www.cesmad.sk/page.php?kat=281
[257] See, https://www.facebook.com/pages/Podporujem-dopravcov-v-štrajku-Mýto-sa-týka-nás-všetkých/226312988873, accessed 17/12/2013

- **Users of the ETS**, based on recent press release by the SkyToll, ETS has 231 287 OBUs in evidence, 72,3 % of which are registered by foreign entities[258]

Other stakeholders that were or are involved with the ETS are not listed, either because they influence only limited part of the ETS (e.g. European Commission, regional governments), or their influence is unknown due to the nature of their connection to ETS (e.g. Slovak Information Service, Military Intelligence, and Financial Authority- allowed access to ETS data by the law).

3. The history of the ETS

In this part we explain history of ETS in Slovakia from legal, political and technological perspective and its current state.

3.1.Political Perspective

The history of ETS in Slovakia is intertwined with development in the Central Europe, where several countries (e.g. Germany, Austria[259]) introduced ETS in 2005 and 2004 respectively. Almost immediately Czech Transport Ministry announced a plan to introduce ETS as soon as possible, also in order to limit impact of transition vehicles that decided to use Czech roads instead of Germany and Austria[260]. Within the next decade all countries in the region introduced toll systems for heavy vehicles over 3.5 tons (Poland[261], Hungary[262], Czech

[258] SkyToll, Press Release, 16/12/2013, available at: http://www.skytoll.sk/download/TS_vyber_myta_november_2013_v1.0_svk_20131216.pdf, accessed 18/12/2013
[259] See http://www.go-maut.at
[260] See: ČTK (Czech Press Agency): Elektronické mýto aj v ČR (Electronic Toll also in Czech Republic), 04/01/2005
[261] See http://www.viatoll.pl/en/heavy-vehicles/news
[262] See: https://www.hu-go.hu/articles/index/3150

Republic[263]). "The policy trend of many countries, especially in eastern Europe, [was] to implement brand new charging systems aimed at financing the building and maintenance of new road infrastructures".[264]

Slovakia soon followed Austrian and German example. In 2005, the Slovak government approved a strategic document on transport policy[265] that envisaged the replacement "of user fees applied on motorways, expressways and selected first class roads with electronic toll system in 2006". However, the introduction of the ETS was delayed till January of 2010 due to political and legal problems. Firstly, the preparation of the ETS coincided with the 2006 parliamentary elections that resulted in a complete change of government. Secondly, although the framework legislation for ETS was approved at the end of 2006 by the Slovak parliament, the public procurement process for the ETS was delayed several times due to complications. The ETS system was one of the first to test the financing through public private partnership (PPP), by which the new government led by the Prime Minister R. Fico planned to finance several large infrastructure projects.

During the preparation phase of ETS several political commentators pointed to the scale of the project (the estimated value of the contract was believed to be around 660 million EURO) and its "attractiveness" for interest groups close to the political parties in the government.[266] These opinions were confirmed by the public procurement itself, in which the National Highway Company (NDS) that procured the system on behalf of the state excluded

[263] http://www.mytocz.eu/index.html
[264] See: Study on economic and social impact of the implementation of Directive 2004/52/CE on interoperability of electronic fee collection in Europe, Final Report, available at: http://ec.europa.eu/transport/themes/its/studies/doc/eets_socio_economic_impact.pdf
[265] The Office of The Government, Transport Policy of the Slovak Republic Until 2015, approved by the Government of the Slovak Republic No. 445 from 8. June 2005, available at http://www.telecom.gov.sk/index/open_file.php?file=mtpt/transport_policy_1.pdf, accessed 03/11/2013
[266] E.g. SME, Video-Editorial, Je šokom, že tender na mýto vyhrala najdrahšia ponuka (It Is A Shock That Most Expensive Bid Won), 06/05/2008, available at: http://komentare.sme.sk/c/3862661/videokomentar-je-sokom-ze-tender-na-myto-vyhrala-najdrahsia-ponuka.html, accessed 09/12/2013

three out of four bids for failing to meet technical requirements and ended up picking the only remaining, and also the most expensive bid for 852,1 million EURO).[267] The procurement is still subject of an ongoing infringement procedure initiated by the European Commission "for breaching European legislation by failing to announce a Europe-wide tender for its electronic road-toll system operator and discriminating against candidates in the tender process".[268] Despite the legal challenge from the EC, and several legal challenges from companies that submitted failed bids, the winning consortium SanToll - Ibertax signed a 14 year contract (with five year option) in January 2009. The contract was based on DBFOT principle (stands for Design – Build – Finance – Operate – Transfer).

The political decision on the ETS received wide political support from all relevant political parties. Overwhelming majority 122 out of 150 MPs supported the original 2007 law on electronic toll collection in the final reading in December 2006.[269] Although the implementation of the ETS, especially the public procurement, was widely criticized by the opposition, mostly in 2010, the year of parliamentary election, the new government of Mrs. Radičová (2010-2012) that replaced the government of Mr. Fico (2006-2010) did not challenge the public procurement and introduced only minor legal changes into the ETS, e.g. lowering of fines and extension of toll roads.

As for the perspective of the watched, the actual introduction of the ETS was met with the massive protests of interest associations that attempted to block main roads both in January

[267] "However, after the contract had been signed with the winner of the tender (the SanToll-Ibertax consortium) on January 13, 2009, several of the tender conditions were changed." See TASR, EC sends reasoned opinion to Slovakia over road-toll system tender, 01/10/2010, available at: http://spectator.sme.sk/articles/view/40309/10/ec_sends_reasoned_opinion_to_slovakia_over_road_toll_system_tender.html, accessed 09/09/2013

[268] See European Commission, Public procurement: Commission calls on Slovakia to respect EU rules for electronic toll collection contracts, 30/09/2010, Available at: http://europa.eu/rapid/press-release_IP-10-1244_en.htm?locale=en, accessed 08/11/2013

[269] See, National Council of Slovak Republic, Voting session, 13/12/2006, available at:http://www.nrsr.sk/web/Default.aspx?sid=schodze/hlasovanie/hlasklub&ID=20159, accessed 09/12/2013.

and February 2010, but without much success. The protests ended after few days. Once again, it is important to stress that these protests were not motivated by the surveillance aspect of the ETS, but by the financial impact of the toll and conviction that the system was not ready. As protesters managed to get something from the government, namely introduction of ticketing system for some roads[270] and temporary suspension of the toll collection on 1st class roads[271], in the end the watched accepted the existence of the ETS. A review of critical responses to ETS system (blockade, use of jammers, avoidance of toll network) is discussed in part 4.

The biggest question from political perspective of the ETS is intertwined with the public procurement and suspicions of foul play by the governing political parties and their business friends.[272] Even in December 2013 the question of the real owners of SkyToll remains unanswered. [273]

[270] The „ticketing" allowed to calculate and collect the toll according to according to the data found in the vehicle logbook or in the vehicle registration certificate. It applied only to four specified transit road sections in Slovakia that were near the border with Czech Republic, Hungary and Poland. The ticketing ended in September 2013. See: Ticketing, available at: https://www.emyto.sk/web/guest/ticketing, accessed 09/12/2013

[271] The toll collection was suspended till March 1, 2010.

[272] See e.g. investigative report by newspaper SME in March 2010, in which daily unsuccessfully attempted to found out who is 90% majority owner of Ibertax (JSC) that owns 100% of the SkyToll. SME, Šéf SkyTollu nás zavádza (Chief Of SkyToll Is Lying To Us), 11/06/2010, p. 12

[273] See e.g. article from weekly Trend that investigated ownership structure of SKYTOLL. Trend, 2013, No. 5, Mýtne prepojenia (Toll Connections), available at: http://www.etrend.sk/trend-archiv/rok-2013/cislo-5/mytne-prepojenia.html, accessed 09/12/2013; or older articles SME, Francúzi z nášho mýta takmer zmizli (French almost missing from our toll), available at, http://ekonomika.sme.sk/c/5859389/francuzi-z-nasho-myta-takmer-zmizli.html, http://www.vyvlastnenie.sk/clanok/a/mytne-prepojenia/, accessed 09/10/2013; SME, Podnikateľa Fila v mýte vysvetliť nevedia (Nobody knows why businessman Filo is involved in toll system), available at: http://ekonomika.sme.sk/c/5850859/podnikatela-fila-v-myte-vysvetlit-nevedia.html, accessed 13/12/2013

3.2. Legal Perspective

The framework legislation for electronic toll system, the Law No. 25/2007 Coll. on Electronic Toll Collection for the Use of Specified Sections of Ground Roads was approved by the Slovak parliament at the end of 2006. The law established basic conditions for introduction of ETS in Slovakia and allowed for public procurement for a system operator. The law also implemented two EU directives, 2004/52/EC on Interoperability of Electronic Road Toll System in the Community and 1999/62/EC on the Charging of Heavy Goods Vehicles for the Use of Certain Infrastructures.

The ETS is legally complex and it is directly intertwined with other laws, e.g. Law on the Railway Police, of which the Toll Police is organizational unit or the law No. 315/1996 Coll. on the Road Traffic, in which toll offences are defined. Beside that, the main ETS law is also implemented by various executive legal acts, e.g. Regulation of the Government No. 350/2007 Coll. stipulating the toll rate amount for the use of specified sections of ground roads, Decree No. 388/2009 Coll. (Toll Order) of the Ministry of Transport, Post and Telecommunications governing details of toll collection or decree No. 441/2011 Coll. of the Ministry of Transport, Post and Telecommunications that specifies the sections of highways, expressways and the 1st class roads in the toll system.

Since its approval in 2006 the main toll law was amended 11 times, mostly by indirect amendments. This is not unusual in Slovak legal system, especially if original law was approved full three years before the ETS launched into the service.

In following sections we look at how the law regulates what kind of data is collected in ETS, what are the purposes, which subjects have the access to the data and whether there were

any changes specific to aforementioned topics between 2006 and 2013. For this we analyzed not only legislation and amendments that were approved and published in the Collection of Laws, but also the legislative process, especially consultation phase in order to find who proposed what and what actually ended up in the legislation. Two general findings from analysis are: 1. No objections to the legal regulation of the ETS were raised by the Slovak Data Protection Agency and,

2. The topic of surveillance (e.g. data collection and retention, data protection, privacy) within the ETS framework was missing altogether from discussions on the governmental and parliamentary level, but also from Slovak media.

What Data Is Collected and For How Long?

There are two types of data that are collected within the ETS. Firstly, it is the data that is collected by the operator electronically, i.e. plate number, technical properties of the vehicle, identification code of on-board unit ("OBU"), distance driven on the toll road, toll rate and information about the vehicle's operator. Second type of the data is collected during the initial registration of vehicle for contract purposes.[274] While there is a specific document on data protection provided by the SkyToll, it informs only about the fact that the data controller of the ETS is the NDS ("National Highway Company), that the data processor is the SkyToll and that the third parties are involved with distribution of OBU units, and therefore, with personal data.[275] While the type of data collected within the ETS is explicitly listed by both

[274] The Vehicle Operator is obliged to provide the following data: the identification details for vehicle operator (e.g.name, address), the first name and surname, date of birth, citizenship and home address of the vehicle driver, the personal ID card or passport number of the Vehicle Driver, the driver's license number of the Vehicle Driver, the identification number of the Vehicle Operator, the TAX ID number of the Vehicle Operator, if assigned, the information, the Vehicle registration number and the country in which the Vehicle is registered, the total Vehicle weight, number of axles and the Vehicle emission class, the information whether the Vehicle is equipped with a device or a modification that could prevent the correct functioning of the On-Board Unit, the estimated total length of Specified Road Sections that the Vehicle Operator plans to drive in the course of a designated time period, the banking details of the Vehicle Operator, the contact details of the Vehicle Operator.
[275] See, SkyToll, Information on the Privacy, available at: https://www.emyto.sk/c/document_library/get_file?uuid=1492eba2-9419-4995-9be6-61ec78310c24&groupId=10136, accessed 08/11/2013

law, and legal contracts provided by the SkyToll, the data retention is limited to citations of data protection law. The data protection law itself is very general when it comes to the data retention. The only explicit period mentioned in documents is the period of six months after which the personal data of the vehicle operator in the ETS are deleted if failing to make the contract within six month. The retention of the data was one of the questions I asked the data processor, SkyToll, when I was interested what happens to the data that are recorded by control gates when there is no hit (e.g. the car is registered and paid toll), the response was that the information is "confidential".

Who Has Access to ETS Data?

The comparison of the first draft of the electronic toll law[276], as discussed by the government in February 2006, with the current wording of the law as of December 2013 shows one important difference. Current law, i.e. §6(7) obliges the ETS operator *to grant live and direct access to all data collected within ETS to the Police and Slovak Information Service (SIS, intelligence agency)*. This part is missing from the 2006 original draft. The proposal to grant access to ETS to the Police was submitted during the second reading of the toll law in December 2006 by coalition MP Mr. Pelegrini, together with several other changes he proposed to the draft[277]. His reasoning was that "the Police needs to control the enforcement of the law, therefore it needs to have an access to ETS data". Although in reaction to his proposal one MP from opposition raised a suspicion that the extensive proposal was in fact prepared by the Ministry of Transport, as it is often the case, the Minister L. Vážny refused

[276] The draft had to be resubmitted due to parliamentary elections in June 2006. In Slovak, available at: http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=6086, accessed 08/11/2013

[277] See Transcipt of the Session of the Parliament, December 2006, 13/12/2006, available at: http://www.nrsr.sk/dl/Browser/Document?documentId=164072

this and acknowledged only extensive consultations with Mr. Pelegrini. The proposal to grant the access to ETS was approved by an absolute majority of MPs (120 out 150).[278]

A year later, in 2007, the Transport Ministry prepared an amendment to the Law on Railway Police in order to establish the Toll Police as an organizational unit. During the consultations on the draft two of the country's intelligence agencies, SIS and Military Intelligence individually proposed an amendment to grant them live and ongoing access to data from ETS. Both demands shared similar arguments, pointing to agencies legal obligations and duties. Only SIS however produced elaborate explanation that argued that direct access to ETS data (e.g. license plates, pictures, localization data, time data) was essential during intelligence operations and could not be substituted with indirect access, as this would "objectively cause noise and faulty data"[279]. The Transport Ministry accepted only the proposal by the SIS and the amendment was approved in the parliament in 2008, the Law No. 86/2008 on the Railway Police.

There are no public data available on how often the access is used by the Police and SIS. Neither official Police statistics, nor annual report by the SIS includes any information. Also, out media analysis did not find any article in which the Police acknowledged the use of ETS data for its operations. I asked about the access in email to the Police, that went unanswered, and to the SkyToll, that called the information, once again, confidential. [280]

[278] See The Recording of the Vote, http://www.nrsr.sk/web/Default.aspx?sid=schodze/hlasovanie/hlasklub&ID=20157, accessed 14/12/2013

[279] Available at: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-77415?prefixFile=m_

[280] See Email conversation with Mr. Bodis, SkyToll, December 2013. Questions asked: 1. How does the access to ETS work, E.g. is Police granted external access, or is member of Police physically present in information centre, or alternatively, access is granted upon a request., 2. Does the SkyToll have any statistics on how often is the access used, e.g. in calendar year?, 3. How does the data retention work within the ETS. E.g. if the control toll gate takes picture of an vehicle, and it is a negative hit (registered and toll is paid), how long does the picture remain in the database.

Access Requests

The general Data protection law regulates the subject access request to ETS data. The aforementioned document on privacy that is available on the website of the EMyto.sk (E-Toll) just mentions existence of the subject access request, with referring to the DP law. However, no templates (online or printed) for requests are available. As for the usage of the right, no public data were available. According to the response from the Slovak DPA, there were no complaints made to the DPA about by legal subjects about the ETS.

3.3. Technological Perspective

The original law on the electronic toll from 2007 was intentionally neutral on the technology that was to be used in the future toll system. All three known toll technologies were acknowledged in the law, therefore opening a possibility for broader competition for future contract. The Slovak ETS uses Global Navigation Satellite System (GNSS) for vehicle positioning together with the cellular mobile system of the cellular network to communicate with an ETS. The On-Board Units used by vehicles integrate all three technologies: satellite GPS module (positioning), GSM/GPRS module (communication within mobile networks) and microwave DSRC module (short-distance communication). The OBUs calculate the position of a vehicle based on time data, the mathematical model of the GNSS satellite movement, and received signals. If the OBU founds that the vehicle is located on a toll road it transmits the data about the vehicle and about the road on which the Vehicle is travelling to the ETS using the GSM (GPRS). Based on the data and the Vehicle parameters (Vehicle

category, weight, number of axles, emission class), the ETS levies a toll according to the rates specified in the decree of the government. [281]

The ANPR technology in the ETS is deployed for dynamic and static control of the vehicles. Dynamic control is performed by the Toll Police, which is authorized by the law to control the compliance with the toll law. The Toll Police uses mobile units equipped with DSRC reader, camera and live access to central information system. The units consist of two crewmembers and are deployed all year around, with one member belonging to the Toll Police and second to Skytoll, the company that operates the ETS. The mobile unit conducts two types of searches, targeted, which are based on the information obtained from dispatcher and random. In case of random searches a unit uses a camera with ANPR capabilities and looks for vehicles that do not have an OBU unit installed. The network of fixed and portable tollgates (over 40) performs static control by the means of DSRC readers and cameras with ANPR capabilities that automatically record data on passing vehicles. The control system works as follows. The DRSC reader and tollgate camera records a vehicle and data are sent for identification of the vehicle and analysis, 2. If system finds, that the vehicle does not have OBU unit installed, OBU is off, or the recorded data matched with database do not correspond with the actual vehicle, it flags the incident, 3. The dispatcher from enforcement back office alerts nearest mobile unit, which stops the vehicle and investigates flagged incident.[282]

[281] Based on ETS Guide, available at: https://www.emyto.sk/c/document_library/get_file?uuid=f8aef32e-7d7c-4fe6-be5a-6ec43a44060c&groupId=10136, accessed 07/10/2013

[282] Compiled from various sources, e.g. TA3, Svet technológií, (World of technologies), 28/11/2009, TV report that investigated technological aspects of ETS system in Slovakia, with special focus on the enforcement, or Bobošík, M., SkyToll: Experiences in Electronic Toll Collection in Slovak republic, presentation, March 2011, available at: http://lists.umn.edu/cgi-bin/wa?A3=ind1105&L=CON-PRIC&E=base64&P=6300812&B=--bcaec547c8ffe8bf3b04a404de06&T=application%2Fpdf; name="ETC_presentation_BUL_110329.pdf"&N=ETC_presentation_BUL_110329.pdf&attachment=q, accessed 09/10/2013.

3.4. Current Situation

While both the political and technological aspects of the ETS remain the same (as of December 2013), there is a significant formal legal change. A new framework law on toll was approved by the parliament in November 2013. When Minister of Transportation J. Počiatek introduced the law in in the parliament, he stressed that the main reason for the law is "protection of 2nd and 3rd class roads from destruction by heavy good vehicles by absolute ban for vehicles on 3rd class roads, extension of toll system for 2nd and 3rd class roads, introduction of absolute liability for toll offences and increase of fines for toll offences.[283] The plan of the ministry is to use a zero-toll on 2nd and 3rd class roads for aggregation of precise data "about movements of trucks in individual regions" and evaluate this data every six months. [284]

The new law replaces the 2007 law. Effective from January 1, 2014 it does not alter legal framework of the ETS dramatically, but it introduces several changes that are relevant for the surveillance aspect of the ETS.[285] First, the law enlists in more detail what kind of data the ETS operator, or third parties collect and process. Secondly, the access to the data from ETS is to be granted not only to the Police and SIS, as it was until now, but also to Financial Administration and Military Intelligence. Both changes were submitted during the consultation phase at the governmental level by Interior Ministry and Defense Ministry. [286] Moreover, the phrasing of the section does not limit the use of the access only to toll offences, as it was in 2007 law. As it was case with the previous 2007 law, proposals to

[283] See Transcript of the parliamentary Session from 16/10/2013, available at file://localhost/o http/::mmserv2.nrsr.sk:NRSRInternet:indexpopup.aspx%3Fmodule=Internet&page=SpeakerSection&SpeakerSectionID=110939&ViewType=content&, accessed 09/12/2013
[284] See Slovak Spectator, 21/10/2013, Changes To Electronic Toll System, available at: http://spectator.sme.sk/articles/view/51739/23/changes_to_electronic_toll_collection.html, accessed 16/12/2013
[285] See Impact Assesment Report, part on Information Society, available at http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=389319, accessed 08/12/2013
[286] See The Draft of Toll Law, available at: http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=22906, accessed 09/11/2013

grant access to ETS data for other enforcement agencies did not get any attention by the media or in later phase by the parliament. Thirdly, the new toll law introduces "absolute" liability for toll offenses in order to increase the enforcement.

Final change brought by the law is not technically part of the law itself. The impact assessment report attached to the draft of the law announces that the new Central Registry for Offences will be established for administration of traffic offences. It will serve primarily as a registry for toll offences, but the report acknowledges that it is going to be used also for other traffic offences and vehicles, outside of the ETS framework, e.g. speeding, reckless driving. In other part of the report it is explicitly acknowledged that the registry will use data gathered by the existing technical infrastructure that is part of ETS enforcement system (e.g. portable and stationary gates, camera systems, radar and laser systems). No other details are yet available on the Central registry. The establishing of Central registry will therefore solve the last problem before introduction of wide surveillance of the vehicles on Slovak roads, as both legal framework, and the technical infrastructure will be in place.

4. Controversies and responses to the ETS

In the following sections we describe controversies that surrounded ETS in Slovakia. With one exception, enlisted controversies are only indirectly connected to the surveillance aspect of the ETS and, as it was in previous text, appear to be directly influenced by the economical motivations of subjects under the surveillance. However, as a matter of fact, several of the controversies (and strategies employed by the subjects) have a direct impact on the surveillance practice.

Alleged Data Mismanagement within the ETS

Few months before the 2010 parliamentary election, and few weeks after the ETS went online, an opposition MP from SDKU, and member of the Parliamentary Committee for Industry, Construction and Transport S. Janiš organized a press conference[287] in which he accused SkyToll of mishandling ETS. He criticized a serious threat to the privacy of citizens that is caused by the malfunctioning ETS, and also the fact that the consortium "owned by mysterious companies with accounts in Cyprus" handles this threat. As an example of problems Mr. Janiš recalled an incident from the committee's investigation into ETS, during which a member of the Committee from coalition Mr. Pelegrini called a CEO of SkyToll and within the five minutes had detailed information about toll paid by one private transport company. "We are going to be under the surveillance by the private company", said Mr. Janiš. In following media reports[288] Mr. Pelegrini did not deny the incident, and explained that he just wanted to check whether one of the spokespersons of the strike, Mr. Polaček, the president of the Union of Slovak Haulers, reported correct information about toll his company paid (3000€ in the first month). He concluded that the incident has to be seen as "undeniable proof that ETS is working properly". The press conference did get traction within the day's news cycle, and was reported by all relevant media, including most popular TV evening news.[289] Despite serious nature of accusations, and the fact that the Transport

[287] See SDKU Press Release, 23/02/2010, Diaľničné mýto – hrozba úniku osobných údajov (Highway Toll- A Threat of Personal Data Leak), available at: http://www.sdku-ds.sk/article/showArticle/278, accessed 08/11/2013

[288] See: SME, 23/02/2010, Štát vyšetruje únik údajov zo SkyToll (State Is Investigating Leak From SkyToll), available at: http://ekonomika.sme.sk/c/5255576/stat-vysetruje-unik-udajov-zo-skytollu.html, accessed 08/12/2013

[289] E.g. HN Online.sk, 23/02/2010, SDKÚ: Mýto ohrozuje súkromie ľudí (SDKU: Toll Threatens Privacy of People), available at: http://hnonline.sk/c1-40704850-sdku-myto-ohrozuje-sukromie-ludi; Nový čas, 23/02/2010, Národná diaľničná sa bráni: S údajmi autodopravcov nie je možné narábať (National Higway Company Says: It Is Not Possible to Manipulate Toll Data), available at: http://www.cas.sk/clanok/153303/narodna-dialnicna-sa-brani-s-udajmi-autodopravcov-nie-je-mozne-narabat.html, accessed 08/11/2013; SME, Štát vyšetruje únik údajov zo SkyTollu (State Is Investigating Data Leak From SkyToll), 23/02/2010, available at: http://ekonomika.sme.sk/clanok.asp?cl=5255576, accessed 03/10/2013; TV Markíza, 23/02/2013, Bezpečnostný systém mýta ohrozuje súkromie ľudí, tvrdí SDKÚ-DS (Security System of Toll threatens Privacy Of People), available at: http://tvnoviny.sk/spravy/domace/bezpecnostny-system-myta-ohrozuje-sukromie-ludi-tvrdi-sdku-ds.html, accessed 07/10/2013

Ministry launched a formal investigation into the alleged leak, the case vanished from media and was not followed legally or politically.[290]

Use of GPS Jammers in the ETS

In March 2010, several weeks after the ETS started, the most popular Slovak weekly Plus 7 dni printed a report titled "Ďalší Škandál" (Another Scandal)[291] on alleged use of GPS jammers that allowed truck drivers to avoid toll. It criticized expensive control system that was, allegedly, unable to cope with cheap GPS jammers that were widely available in e-shops in UK, Poland and Czech Republic. The reporters successfully tested a jammer with anonymous transport company. The article also pointed to the fact that the police at the moment did not have appropriate technical equipment to handle jammers. Various media outlets picked up the story.[292] Daily SME published several articles over short period that investigated further and also asked for comments from NDS, the Police and the SkyToll representatives. While NDS refused to comment, SME managed to interview the Chief of Toll Police who said that he was not a person to comment and "that he never heard about the GPS jammers".[293] A popular online car section of SME also produced a nine-minute video segment on jammers that explained their use. A software engineer explained that the use of jammers was nothing new in Slovakia and that his company had to solve problems of drivers that were avoiding GPS surveillance by their bosses in transport companies by using jammers. The report avoided explicit mentioning of the ETS, and ended up with statement by press officer from Telecommunication Office of Slovakia, who stressed repeatedly, that any

[290] Paradoxically, in the 2011 the political party that uncovered the "data leak scandal", SDKU, at that time coalition party, nominated two former managers from SkyToll to high managerial positions within the central government. See Hospodárske Noviny, 29/09/2010, SDKÚ vsádza na ľudí z mýtnej firmy (SDKU Bets on The People from Toll Company), available at: http://hnonline.sk/c1-46665110-sdku-vsadza-na-ludi-z-mytnej-firmy, accessed 09/12/2003

[291] See, Plus Sedem Dní, Ďalší škandál (Another Scandal), 26/10/2010, available at: http://www.pluska.sk/plus7dni/vsimli-sme-si/dalsi-skandal.html, accessed 03/11/2013

[292] See, e.g. most popular tabloid, Nový Čas, Porazí miliónové elektronické mýto rušička za 80 eur?! (Will ETS for Millions Be Beaten by Jammer for 80 EURO?), 27/03/2010

[293] See SME, Mýto vraj kamióny obchádzajú rušičkami, (Toll Is Allegedly Avoided by the Use of Jammers) , 26/03/2010, http://ekonomika.sme.sk/clanok.asp?cl=5302262, accessed 09/12/2013

use of jammers was an offence punishable by heavy fine, both in Slovakia and EU.[294] A few weeks later SME published another article on the use of GPS jammers.[295] The article cited an official from one of the interest groups who confirmed that he also has information about use of the jammers and pointed to the fact that this is "unfair for all those who are paying dutifully". The newspaper also obtained, from anonymous source, a report about test on efficacy of the ETS, which concluded that out of 12 control gates only one was functioning and that the system was unable to deal with the GPS jammers. Both the NDS and the SkyToll refused to comment. In follow-up article next day[296], the SkyToll representative pointed out to the fact that jammers were illegal and that the company knew how to "handle invisible cars". The Toll Police refused to provide any data on the enforcement of the ban. This series of articles was last one that investigated use of jammers in the ETS. Moreover, a change of communication style is visible from the Toll Police. The Police is more proactive since 2011 and informs periodically[297] about its enforcement within the ETS: e.g., in 2012 the Toll Police, together with the Telecommunications Office of Slovakia performed 87 operations that found 26 jammers, same amount that in 2011.[298] It is impossible to gather hard data on the scale of the use of the GPS jammers in the ETS. Media analysis provided only anecdotal evidence; the official data from police include dozens of cases for 2011 and 2012. Several comments under the theme "Bad Companies" on Profivodic.sk, an site for

[294] See: SME, Vymaže rušička auto z cesty (Will Jammer Erase Car from the Road?), 05/04/2010, available at: http://auto.sme.sk/c/5315032/vymaze-rusicka-auta-z-ciest.html, accessed 06/10/2013

[295] See SME, Rušičky z mýtnych ciest nezmizli (Jammers Still on Toll Roads), 30/05/2010, available at: http://s.sme.sk/r-rss/5399308/ekonomika.sme.sk/rusicky-z-mytnych-ciest-nezmizli.html, accessed 09/10/2013

[296] Sme, SkyToll: rušičky musíte udať (SkyToll: You Have To Inform the Police About Jammers), 01/06/2010, available at: http://ekonomika.sme.sk/c/5401076/skytoll-rusicky-musite-udat.html, accessed 09/11/2013

[297] See video of police operation, available at: http://www.youtube.com/watch?v=50WmlX2oHW8, accessed 09/11/2013 or articles: SITA, Polícia hľadala rušičky, kamionisti nechcú platiť mýto (Police Looking For Jammers, Truck Drivers Avoid E-Toll), 14/08/2012, available at: http://www.webnoviny.sk/slovensko/policia-hladala-rusicky-kamionisti/531233-clanok.html?from=suggested_articles, accessed 09/09/2013; Telecommunications Office, TÚ SR a polícia odhalili používanie rušičiek (TU and Police Uncovered Use of Jammers), 22/03/2011,available at: http://www.teleoff.gov.sk/index.php?ID=4041, accessed 09/10/2013

[298] SME, Kontroly rušičiek vlani odhalili aj celú kolónu nákladných vozidiel (Last Year's Control of Jammers Also Uncovered Fleet of Trucks), 27/2/2013, available at: http://auto.sme.sk/c/6716398/kontroly-rusiciek-vlani-odhalili-aj-celu-kolonu-nakladnych-vozidiel.html, accessed 03/12/2013

professional drivers, also point to the existence of the companies where management forces drivers to avoid toll by using the jammers.[299] While the GPS jammers still remain easily obtainable via Internet[300], websites that sell them include a legal disclaimer about their ban and sole legal responsibility of the buyer.

Protests of Haulers during the launch of the ETS[301]

In December 2009, ČESMAD, the biggest interest group representing haulers in Slovakia, called on the Transport Ministry to propose lowering of excise taxes on motor oil in order to compensate introduction of the ETS. A few days before the official launch of the ETS in Slovakia, dozens of Slovak haulers that were unsatisfied with efforts of the ČESMAD, established the Union of Slovak Haulers and called on the Transport Ministry to delay launch of the ETS, as it was "not ready yet".[302] They also announced that they were prepared to bloc main border transit in January, if the Ministry does not accept some of their demands.[303] In January, the Union launched an information campaign and a petition demanding various changes in the ETS, a reduction in excise taxes on motor fuel and decreases in road tax rates. In the following weeks the Union organized several protests across Slovakia, with main one in Bratislava, where dozens of trucks blocked several main roads. All media reported the blockade, and in the election year it caught attention of both the government and the opposition. It ended after few days after several rounds of negotiations between the government and various interest groups. The Prime Minister R. Fico announced that his government will accept some of the demands from haulers associations and business

[299] See Profivodic.sk , Discussion Topic, Neseriózne Firmy (Bad Companies), available at: http://www.profivodic.sk/node/355?page=1 , accessed 08/12/2013
[300] E.g., http://www.heureka.sk/?h%5Bfraze%5D=rušička, accessed 12/12/2013.
[301] Citing from Bertelsmann Transformation Index Country Report for 2012, "Protest movements have been active, but usually without great success. The only recent exception was the massive protest at the beginning of January 2010, organized by truckers in connection with Slovakia's new electronic toll collection system. The government acceded to most of their demands, cutting the excise tax on diesel fuel and adjusting the e-toll collection system". The whole report is available at: http://www.bti-project.de/laendergutachten/ecse/svk/2012/, accessed 23/10/2013
[302] See Dopravcovia.wbl.sk, available at:http://www.dopravcovia.wbl.sk, accessed 09/12/2013
[303] SITA, 22/12/2009, Haulers Prepare Last-Minute Protest against High Toll.

community (e.g. Chamber of Commerce), which included introduction of the ticketing system for several roads near state borders, lowering of excise taxes on motor oil and temporary suspension of toll payments on 1st class roads.[304] The Transport Minister Ľ. Vážny also survived a no-confidence vote in the parliament after the opposition demanded his resignation for troublesome implementation and launch of the ETS.

During the protests of transport companies the media informed about the case of a destroyed tollgate at a 1st class road near Bratislava.[305] The Prime Minister R. Fico mentioned the incident during his press briefing, saying, "This is a road to hell". Mr. Fico warned everyone who is going to destroy tollgates to be prepared for consequences. Soon after another tollgate was destroyed, with its hardware stolen.[306] It was the last incident.

Although the Union of Slovak Haulers remained in strike emergency for remaining of the year, unsuccessfully sued SkyToll for faults of the ETS in 2010[307] and threatened with another blockade in 2011, the new leadership of the Union changed their tactics and started to concentrate their efforts on more traditional lobbying activities to demand favorable conditions for hauler business in Slovakia[308]. In an example of such effort, the interest groups for haulers were extensively consulted about the new law on toll introduced in 2013,

[304] SITA, 11/01/2009, Haulers Win a Promise of Lower Diesel Tax, Zero Toll on Some Roads.

[305] SME, Podpílili mýtnu bránu, zasahovala do cesty (Someone destroyed TollGate), 28/01/2010, available at: http://auto.sme.sk/c/5213337/podpilili-mytnu-branu-zasahovala-do-cesty.html, accessed 08/09/2013

[306] SME, Napriek Ficovej hrozbe podpálili ďalšiu mýtnu bránu (Despite PM's Warning They Destroyed Another TollGate), 02/02/2013, available at: http://trnava.sme.sk/c/5221258/napriek-ficovej-hrozbe-podpalili-dalsiu-mytnu-branu.html, accessed 09/09/2013

[307] See, Únia dopravcov Slovenska žaluje SkyToll (Union of Slovak Haulers Sues SkyToll, 18/11/2010, available at: http://www.pluska.sk/ekonomika/slovenska-ekonomika/unia-autodopravcov-slovenska-zaluje-skytoll.html, accessed 08/12/2013

[308] See the interview with the new President of the Union of Slovak Haulers, available at: http://uniadopravcov.wbl.sk/PRESS.html, accessed 09/12/2013

in which the government compromised on a proposal to increase toll rates automatically with the inflation, which interest groups refused.[309]

AVOIDING TOLL ROADS

Probably most visible governance problem of the ETS[310] has to do with deliberate avoiding of toll roads by trucks by using roads of 2nd and 3rd class.[311] This resulted in an increase of the traffic by vehicles driving through communities, and damages to properties and local road infrastructure. All national governments acknowledged the existence of the problem, and attempted to use legal, economical and informational instruments to solve it, without being able to produce a working solution so far. The problem also points out to the complicated problem solving when it includes three levels of the government, as the problem is local, the 2nd and 3rd class roads belong to the regions, but it is only the national government that has policy instruments to solve it. To complicate the solution to the problem even more, three different national governments were in the office between 2010 and 2013.[312]

---

[309] Slovak Spectator, Changes to electronic toll collection, 21/10/2013

[310] A few weeks after launch of the ETS the members of regional governments informed at the press conference that avoiding of the toll roads is already causing a significant damage to local roads. See: Aktuality.sk, Kamióny ničia cesty (Trucks Are Destroying Roads), 03/02/2010, available at: http://www.aktuality.sk/clanok/155978/kamiony-nicia-cesty-hovori-predseda-ttsk-i-starostovia/, accessed 07/12/2013

[311] The problem itself was subject of dozens of media reports, e.g. SME, Dvoriankam ničia život kamióny (Dvorianky Destroyed by Trucks), 09/08/2013, available at: http://www.sme.sk/c/6897109/dvoriankam-nicia-zivot-kamiony-obyvatelia-stracaju-trpezlivost.html, accessed 07/12/2013; Nový Čas, Trápenie obyvateľov Mýtnej (Suffering of Mýtna), 11/07/2013, available at: http://vas.cas.sk/clanok/8220/trapenie-obyvatelov-mytnej-domy-im-padaju-na-hlavu-nicia-ich-kamiony.html, accessed 07/12/2013; Pluska.sk, Kamióny spôsobujú praskanie domov (Tracks Are Causing a Damage To Houses), 14/10/2010, available at: http://www.pluska.sk/slovensko/regiony/kamiony-sposobuju-praskanie-domov.html, accessed 09/12/2013; Sme.sk, Šalania žiadajú spoplatnenie cesty ktorá prechádza mestom (People of Šala demand Toll Road), 15/11/2011, available at: http://nitra.sme.sk/c/6139653/salania-ziadaju-spoplatnenie-cesty-ktora-prechadza-mestom.html, accessed 09/12/2013

[312] Probably most elaborate effort to map a complicated workings of the government in Slovakia in this instance is provided by the leader of petition committee in village Dvorianky. Mr. J. Vitkovič, who attempts for several years to solve the problem by allerting state authorities. In this blog post he explains how two ministers promised a solution, to no avail, and currently five different sections of the Transport Ministry review his demands. See http://janvitkovic.blog.sme.sk/clanok.asp?cl=342514&bk=50796, accessed 09/12/2013

In August 2012, the newspaper SME published, as a part of "Personalities Make Newspapers series", a long report[313] about the problem. Slovak singer and actress S. Tobias reported her personal experience with life in the village that was devastated by the transition trucks avoiding toll. This story was similar to other stories from Slovakia in places where toll roads run parallel with the local ones. The article reported about problems of several Slovak villages that struggled with transiting trucks that used their roads in order to avoid toll. The actress talked about her experience and frustration when trying to solve the problem with regional and national authorities. A video attached to the report showed the experience of Lednice, where it took two and a half years to get a no entry traffic signs from state authorities. Several other places were mentioned in the report, citing people vocalizing their frustration about heavy traffic and destruction of their properties. "If we move to the front room, you will feel the ground shaking. It is worst on Sunday evening. We cannot sleep. It is depressive", said one of the villagers for the newspaper. The article also discussed a problematic coordination as the administration of local roads belonged to regional governments, but enforcement and ETS to the national government. In 2011, the Transport Ministry discussed the proposal of a nation-wide ban of heavy vehicles from local roads, but decided instead to increase the number of no entry signs in several problematic areas. After the 2012 parliamentary elections, the New Interior Minister R. Kaliňák acknowledged that there has to be a more coordinated effort to solve the problem that will also include legislative changes. The problem of avoiding the toll roads is addressed in the new 2013 law. The law extends ETS to roads of 2nd and 3rd class (with zero toll) and once again, significantly increases fines for use of these roads. The extension will allow for better monitoring of the traffic and increased enforcement that will cover more roads.

[313] SME, Kamionisti šetria na mýte a ničia domy i život v obciach (Trcks save on toll and destroy properties and life in villages), 24/08/2012, available: http://www.sme.sk/c/6509458/kamionisti-setria-na-myte-a-nicia-domy-i-zivot-v-obciach.html, accessed 09/11/2013

The change in the new 2013 law confirmed that current enforcement was not able to handle the scope of this problem, despite repeated complaints from communities, regional politicians and media. An interesting case of the community effort to offer rich evidence of the scale of the problem to the state authorities could be found in village Dvorianky[314], where citizens organized an informal group that systematically monitored the situation. In order to provide precise data[315] to state administration on traffic and types of vehicles that were using their road, they used infrared cameras. They have their own Youtube channel with video footage of transiting trucks in various time periods[316], a blog[317], a webpage[318] and a Facebook account[319]. In 2013, after months of complaining to various level of the government, they finally achieved that the road that transits their village will be included in ETS from January 2014. However, as a blog post of petition chairman argues, the doubts remain, as the toll for using their road will be cheaper compared to a parallel highway.[320]

5. Conclusion

The Electronic Toll System in Slovakia was launched as the state of the art tolling service with one of the largest coverage of roads in Europe. However, the preparation of the project and its implementation were confronted with various problems, some of which have wider implications for accountability, transparency and governance in Slovakia.

---

[314] The case was reported by several media outlets, e.g. SME, Dvoriankam ničia život kamióny, obyvatelia strácajú trpezlivosť (Life In Dvorianky Destroyed By Trucks, People Are Loosing Patience), available at: http://www.sme.sk/c/6897109/dvoriankam-nicia-zivot-kamiony-obyvatelia-stracaju-trpezlivost.html, accessed 09/10/2013; For complete media monitoring on Dvorianky see the webpage of petition committee, http://dvorianky5.webnode.sk/clanky/

[315] See, http://dvorianky5.webnode.sk/stav/kamiony-vikend/, accessed 08/12/2013

[316] Available at: http://www.youtube.com/playlist?list=UUKKU2fb7mZqcmtYmocEDSkg

[317] SME blog, http://janvitkovic.blog.sme.sk/c/343488/Otrasy-24-hodin-denne-Praskaju-rodinne-domy.html, Accessed 09/12/2013

[318] See http://dvorianky5.webnode.sk

[319] https://www.facebook.com/jan.vitkovic.96

[320] See SME blog, 13/12/2013, Zázrak sa nekoná (The Miracle Is Not Happening), available at: http://janvitkovic.blog.sme.sk/c/344481/Zazrak-sa-nekona-spoplatneny-usek-I79-nie-je-paralelny.html - t2, accessed 13/12/2013

The ETS was one of the first large scale projects that used public-private partnership. It is the private company, SkyToll that was awarded a massive contract to prepare and operate ETS with potentially massive surveillance capability. With the amount and the length of the contract, and possibilities of the system one would expect that the state ensured that the additional checks are in the place for greater accountability and transparency of the project. The opposite is true. The public procurement for the system operator from 2008 is still under investigation by the European Commission after the NDS, under direct supervision of the Transport Ministry, decided to disqualify three bids from the procurement and awarded the contract to the only remaining, and the most expensive bid from the consortium Ibertax-SanToll.

Other red flags remain raised due to unknown ownership of the parent company of the SkyToll, the Ibertax. While several reports pointed out to the proximity of winning companies to the government of the Prime Minister Fico, the next government of Mrs. Radičová did not manage to shed more light into murky ownership of Skytoll. When Mrs. Radičová (2010-2012) negotiated changes in the ETS contract with Skytoll in order to restructure some of the payments, even she was forced to acknowledge not to have precise information why certain people are representing SkyToll during the negotiations with her government. With the Prime Minister Fico (2012-) back in the office, together with all the political actors that were directly responsible for the ETS (e.g. former Transport Minister L. Vážny, currently serves as Vice PM For Strategic Projects), the question of the real owners of the SkyToll remains unanswered, despite best efforts of the media. The problem here is not only one of the transparency, where the state is unwilling to uncover who was awarded biggest public contract in Slovak history, but also of the accountability, where interests of the political actors seem to be aligned more with their sponsors than with those of the public.

While Slovakia had its amount of big scale projects with allegations of corruption, the ETS is unique as it is the first one with massive surveillance potential. As we explained in the report, the scope of the ETS increased significantly since the 2010 launch and will cover most of the roads in Slovakia from 2014. While it remains to be seen whether the increase in scope of roads covered by the ETS will be supplemented by necessary investment (financial and personal) into ETS enforcement, it is obvious that the state intents to use surveillance capabilities of the ETS outside its original purpose. This is demonstrated not only by the access to the ETS data that was guaranteed to intelligence agencies, the Police and Financial Authority in the 2013 law, but also by the other legal changes that allow to use ETS data for other purposes than only ETS enforcement. Moreover, the government plans to use ETS data in two databases to be launched in the near future. All these changes were approved through the regular legislative process, and were accepted without any opposition from state agencies, the opposition parties, interest groups and the media. This is where the lack of advocacy for privacy issues is most visible. Theoretically, one would expect Slovak Data Protection Agency to play significant role during preparation of ETS, its implementation and current changes. The opposite is the case. The agency did not raise a single objection during the consultations of the 2007 law and the 2013 law. When in 2010 a MP from opposition alleged that coalition MP was able to obtain personal data from the ETS "after one phone call to the director of SkyToll", the DPA did not launch any investigation into the matter. While this may be an exception, our report for WP5 also found the Slovak DPA is a technocratic agency that rarely enters public debates and controversies.[321] Other traditional advocates, e.g. NGO's are historically more focused on transparency and fight against the corruption. The lack of the awareness is ideal for function creep of the ETS that we are witnessing these days. What is more worrying is that there are several E-Government projects in the preparation[322] that may soon exponentially increase massive surveillance in

[321] You will not find any official reponses to Snowden scandal, or new governmental projects from Slovak DPA.

[322] It has to be said that within relatively short period Slovakia introduced, or is to introduce several large public projects that have a serious surveillance potential, from omnipotent police cars, ID cards

Slovakia. If combined with tendency for non-transparent public procurement, the life of Slovaks citizens and companies may end up being watched over by omnipotent financial groups that already seem too big to fail.

Resources (media sources are cited in endnotes)

Národná diaľničná spoločnosť, 2010, Report: Multi-lane Free-flow Electronic Tolling in the Slovak Republic, available at: http://www.schild-partner.com/SuP/Road_Pricing_&_Electronic_Tolling__Free_Flow,_satellite_based_tolling_systems___Schild_&_Partner_files/Multi-Lane Free-Flow Electronic Tolling in the Slovak Republic.pdf, accessed 08/10/2013

Bobošík, M., SkyToll: Experiences in Electronic Toll Collection in Slovak republic, presentation, March 2011, available at: http://lists.umn.edu/cgi-bin/wa?A3=ind1105&L=CON-PRIC&E=base64&P=6300812&B=--bcaec547c8ffe8bf3b04a404de06&T=application%2Fpdf;name="ETC_presentation_BUL_110329.pdf"&N=ETC_presentation_BUL_110329.pdf&attachment=q, accessed 09/10/2013

Government Of Slovakia, Transport Policy in Slovakia, Document No. 445 from 8. June 2005, available at: http://www.telecom.gov.sk/index/open_file.php?file=mtpt/transport_policy_1.pdf, accessed 09/10/2013

with chips, electronic monitoring of prisoners to E-Health card that is to be introduced in 2016. Almost all of these initiatives are to be co-financed from EU cohesion funds.

Ernst & Young, Study on economic and social impact of the implementation of Directive 2004/52/CE on interoperability of electronic fee collection in Europe, Final Report for EC, available at: http://ec.europa.eu/transport/themes/its/studies/doc/eets_socio_economic_impact.pdf , accessed 09/10/2013

European Federation for Transport and Environment, A Price Worth Paying: A guide to the new EU rules for road tolls for lorries Second edition, June 2007 , Available at: http://www.transportenvironment.org/sites/default/files//docs/Publications/2007/2007-06_price_worth_paying_v2.pdf, accessed 09/09/2013

IRISS WP3 ANPR UK CASE STUDY

Prepared by Clive Norris USFD

1. Introduction

This report examines the British Police's use of the Automatic Number Plate Recognition (ANPR) technologies since the mid 1970s when its potential as a policing tool was first investigated. It will outline the history of the development of the National ANPR Strategy, which has led to a network of 8000 cameras feeding into to a centralised police database. It will then consider its current operational use, before describing the key controversies that have arisen surrounding ANPR. In particular it will examine ANPR's role in the policing of political protest; attempts by citizens to force the police to disclose the location of the cameras; a legal challenge by activists as to the legality of the camera network; and an attempt by the police to subject a predominantly Muslim community to blanket ANPR surveillance coverage. It will then reflect on the implications of these controversies and their resolutions for our understanding of surveillance and democracy.

This report has drawn upon the following:

- All newspaper articles mentioning ANPR published in The Guardian from 2004 – 2014;
- All online BBC news reports mentioning ANPR from 2004 – 2014;
- All articles mentioning ANPR on the Register web site 2004 – 2014;
- Selective on-line news reports from The Daily Telegraph, The Daily Mail and the Daily Express;

- Key policy documents issued by ACPO;
- Key policy documents issued by the ICO;
- The legal judgments issued by Information Tribunal;
- The Web sites of the key pressure groups with an interest in ANPR: Privacy International; Big Brother Watch, No CCTV; and FitWatch;
- Freedom of Information requests related to ANPR[323];
- The key scholarly articles.

2. Key Players in the ANPR Story

ACPO: The Association of Chief Police Officers: "ACPO leads and coordinates the direction and development of the police service in the United Kingdom" and was responsible for the development and implementation of the national ANPR Strategy 'Denying Criminals the use of the Roads.'[324] As a private company, its constitutional status has been the subject of recent debate and its role set to change.[325]

ICO: "The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals". [326]

PRIVACY INTERNATIONAL: Is an international privacy rights pressure group which has consistently campaigned against the diffusion of ANPR technologies.[327]

[323]https://www.whatdotheyknow.com/
[324]http://www.acpo.police.uk/
[325]http://blogs.telegraph.co.uk/news/douglascarswellmp/100266321/its-game-over-the-association-of-chief-police-officers-thank-god-for-that/
[326] http://ico.org.uk/about_us
[327] https://www.privacyinternational.org/about-us

NO CCTV: Is a single issue campaigning group which seeks to challenge the spread of CCTV surveillance in the UK under the banner "campaigning against CCTV surveillance and beyond".[328] Although its primary focus is open street CCTV systems, it has been particularly vociferous in its opposition to the expansion of ANPR surveillance.[329]

THE GUARDIAN NEWSPAPER: The national 'left of centre' newspaper The Guardian has played a major role in drawing attention to the surveillance activities of Britain and its 'five eyes'[330] collaborators, particularly America[331]. In particular, it has supported the journalist S A Mathieson in his campaign to force the police to reveal the location of ANPR cameras.[332]

THE DAILY EXPRESS AND DAILY MAIL NEWSPAPERS: Both 'right of centre' newspapers have been vociferous in their opposition to speed cameras and any application of CCTV or ANPR cameras which are used to enforce the law against traffic violations. They tend to characterise any attempt to enforce the law in relation to motorists as being motivated by the desire of local authorities to generate revenue via a 'stealth tax'.

BIG BROTHER WATCH: "Big Brother Watch was set up to challenge policies that threaten our privacy, our freedoms and our civil liberties, and to expose the true scale of the surveillance state."[333] Along with 'No CCTV' and 'Privacy International', Big Brother Watch challenged the legality of ACPO's National ANPR Strategy in a complaint to the ICO.[334]

---

[328] http://www.no-cctv.org.uk/default.asp
[329] http://www.no-cctv.org.uk/whats_wrong_with_anpr.asp
[330] http://www.bbc.co.uk/news/world-europe-24715168
[331] http://www.theguardian.com/world/2014/apr/20/guardian-pulitzer-prize-snowden-rusbridger
[332] http://samathieson.com/sa-mathieson/category/privacy/anpr/
[333] http://www.bigbrotherwatch.org.uk/about
[334] http://www.theguardian.com/uk/2011/jul/28/royston-under-surveillance-police-cameras

FITWATCH: A pressure group that campaigns against police surveillance tactics at sites of public demonstration and protest. In particular, it has highlighted what they see as the harassment and intimidation of lawful protesters by police Forward Intelligence Teams (FITS) and has documented the use of ANPR technologies to monitor protestors.[335]

This report is going to focus primarily on the Police use of Automatic Number Plate Recognition (ANPR) as this has been the area where there has been the most controversy. However, it is worth briefly outlining some of the key non-police uses of ANPR systems. In the UK, ANPR is now used widely to monitor vehicular access to public and private sites and their associated car parking spaces. It is increasingly used to monitor and enforce payment for car parking, in a range of public and private schemes. Here the scheme operators can gain access to the Driver and Vehicle Licensing Agency's (DVLA) database of registered keepers, 'with the reasonable cause of broken contract for parking on private land'. It is also being increasingly used by local authorities to enforce bus lane restrictions and other infringements of traffic laws. In a similar way that the uses of speed cameras aroused fierce opposition from certain sections of the British Press, local authority use of ANPR is also now a subject of much hostile journalism. For instance, under the headline, 'Those sneaky council spy cars fleece drivers of £32million a year... but now motorists are fighting back', *The Daily Mail* newspaper reported*:*

> that in the 12-month period between November 2012 and October 2013, more than 110 spy vehicles used by councils in England and Wales resulted in 330,000 penalty charge notices for parking offences and so-called 'moving traffic violations'. These would have raised £32 million, if paid in full.[336]

[335] http://www.theguardian.com/commentisfree/2010/nov/16/fitwatch-website-closed-police
[336] http://www.dailymail.co.uk/news/article-2597460/Those-sneaky-council-spy-cars-fleece-drivers-32million-year-motorists-fighting-back.html

3. The Development of ANPR for Policing

A brief history of the police development and deployment of ANPR technology:

- 1976: The Government's Home Office Scientific Development Branch began working on the development of ANPR Technology.[337]

- 1980: It was reported in the Annual Report of Her Majesty's the Chief Inspector of Constabulary that a field experiment was to be conducted to test the viability of automatic number plate reader technology being linked to the Police National Computer. The main use was declared to be the identification of stolen vehicles.[338]

- 1982-84: Between July and October 1982 police-sponsored trials occurred at the approach to London's Dartford Tunnel road crossing of the river Thames. These were superseded by trials of a more advanced system on the main national motorway, the M1, which could match a number plate against the database of suspect vehicles in 15 seconds. Further work was being undertaken to reduce the time to complete the matching process to one second. [339]

- 1996: The City of London's 'Ring of Steel' was the first major application of ANPR as a counter terrorism measure. It was set up in the wake of the Bishopgate's bombing, which killed one person, injured forty and caused hundreds of millions of pounds worth of damage in the heart of London's international financial district. Rather than 'steel', the system consists of cameras situated at each of the entry points into the

[337] No CCTV (2013) *What's Wrong With ANPR?* http://www.no-cctv.org.uk/whats_wrong_with_anpr.asp, p.2
[338] ibid.
[339] BSSRS (1985) *TechnoCop: New Police Technologies*, BSSRS Technology of Political Control Group, Free Association Books, 1985, p. 50.

City. Since 1996, every vehicle that enters the square mile of the City of London has had its licence plate read by the cameras. This information is then automatically checked, in real time, against a number of databases that contain details of the vehicles of suspected terrorists. If a match is made, an alarm is sounded and officers can be deployed to investigate the suspicious vehicle further.[340]

- 2001-02: Project Spectrum - In response to the 9/11 bombing of the World Trade Centre in New York and the subsequent war on terror, the first nationally co-ordinated deployment of ANPR in England and Wales was initiated. Under the Crime Reduction Programme the Home Office allocated £4.65 million to provide each force in England and Wales with one mobile ANPR unit and associated back-office facility.[341]

- 2002-03: Project Laser was a six-month pilot of fixed ANPR cameras in nine police forces.[342] The aim of the pilot was to gather information on the operation and impact of ANPR-enabled intercept teams, to inform policy and assess the potential of a national roll out. In the trials, the teams "stopped 39,188 vehicles, arrested over 5000 persons (of which only 20% were for driving related matters) and took a further 45,000 actions. These included issuing verbal advice or a fixed penalty, or requesting that vehicle documentation, such as MOT certificates and vehicle insurance, be presented at a police station".[343]

---

[340] Graham, Stephen (2004). *Cities, War, and Terrorism: Towards an Urban Geopolitics*. Wiley. pp. 281–284.

[341] http://www.cjp.org.uk/news/archive/driving-crime-off-the-roads-automatic-number-plate-recognition-systems-launched-nationwide-14-11-2002/

[342] Project Laser involved nine forces. It ran for six months from 30th September 2002 to March 2003.

[343] PA Consulting (2004): PA Consulting (2004) *Engaging criminality – denying criminals the use of the road*, PA Consulting Group, London. p14

- 2003: London Congestion Charging introduced to central London. The area in which charges apply is a zone measuring 21 square kilometres with a total of 203 entry and exit points.[344] Road signs alert motorists when they enter the charging zone. There are no tollbooths, barriers or tickets - instead, drivers pay to register their vehicle number plates on a database, and a network of nearly 700 cameras records their entry into, movements within and, exit from the zone. The number plates are matched against the database. If a vehicle is registered as having paid by midnight on the day of travel, then the data is erased. If the vehicle is identified as having not paid the charge then the registered owner is automatically sent a fixed penalty notice. The address is obtained from a link, which provides access to the DVLA database of registered keepers.[345]

- 2003: Project Laser is extended and the pilot study increased to 23 forces, part-funded by money from the fixed penalty fines generated from motoring offences captured by the system. During the 13 months of Laser 2, "ANPR cameras read approximately 28 million VRMs[346] of which over 1.1 million (3.9%) resulted in a hit. In total, the ANPR intercept teams stopped 101,775 vehicles (9.2%) of these vehicles as a result of ANPR hits".[347] According to the, then home secretary, David Blunkett, the outcomes from the pilot were impressive and the "Home Office estimates that a national roll-out of ANPR would lead to approximately 24,400 additional offences being brought to justice each year – a significant contribution of around 15% towards meeting the Government's target for offences brought to justice."[348]

---

[344] Transport for London (TfL), Congestion charging: Impacts monitoring, Second Annual Report, April 2004. http://www.tfl.gov.uk/assets/downloads/Impacts-monitoring-report-2.pdf

[345] http://news.bbc.co.uk/1/shared/spl/hi/uk/03/congestion_charge/exemptions_guide/html/what.stm

[346] VRM: Vehicle Registration Mark

[347] Op. cit., PA Consulting 2004, p. 61

[348] Blunkett, D., foreword to PA Consulting 2004 *Driving Down Crime, Denying Criminals use of the Roads*, PA Consulting Group, London.

- 2005: The Association of Chief Police Officers (ACPO) published their National ANPR Strategy "Denying Criminals the Use of the Roads" 2005/2008.[349] The strategy consisted of four key components: the setting up of a national network of ANPR-capable cameras; the creation of dedicated intercept teams in each force; real time linkages with the DVLA database of registered keepers of motor vehicles and to the databases contained on the Police National Computer (PNC);[350] and the creation of a National ANPR Data Centre to house a database capable of storing 35 million ANPR reads per day.[351]

- 2007: The Home Secretary, Jacqui Smith, granted The Metropolitan Police force and Transport for London exemption from the Data Protection Act to allow the real time transfer of data from the London Congestion charge system to the Metropolitan Police. Police were previously able to request specific footage from those cameras for reasons of national security. However, given that data is erased once payment has been confirmed, this limited the potential use for police purposes.[352] The certificate allowed for the blanket transfer of real time data to be stored and processed by the police but only for the purposes of matters of national security and not for general policing purposes.[353]

4. The current capabilities of the system

[349] ACPO - Association of Chief Police Officers – (2005) ANPR Strategy for the Police Service 2005-8: Denying Criminals the Use of the Road, London ACPO
[350] Additionally the system was linked to local force databases, the MIDAS (Motor Insurance Database) and counter terrorism databases.
[351] ACPO (2005) op. cit., p. 18.
[352] Metropolitan Police Service (MPS), (2007) Briefing Note for the Information Commissioner in relation to Project 28 on behalf of the Metropolitan Police Service. A redacted version available at: https://www.whatdotheyknow.com/request/175160/response/462279/attach/12/Briefing%20Note%20for%20the%20Information%20Commissioner.pdf.pdf

[353] http://www.out-law.com/page-8309

The ANPR system really works in two distinct ways: to enable the real time interception of 'suspect' vehicles and through the generation of intelligence profiles based on the analysis of the stored data.

Real-time interception works in the following way: ANPR “reads” Vehicle Registration Marks – more commonly known as number plates – from digital images, captured through cameras located either in a mobile unit, in-built in traffic vehicles or via CCTV. The digital image is converted into data, which is processed through the ANPR system. This system is able to cross reference the data against a variety of databases including the Police National Computer (PNC), local force intelligence systems and other related databases, for example, that of the Driver and Vehicle Licensing Agency (DVLA). Once the data has been cross-checked against these databases – a process that takes around 1.5 seconds to complete – information about the vehicle, its registered owner and driver appears on a computer where it is evaluated by ANPR officers. If the information supplied via the ANPR system alerts officers to an offence or relevant intelligence on a vehicle, the vehicle will be stopped to allow officers to investigate further. ANPR officers acting as “interceptors” also use their own observations to stop other offenders not highlighted by the system. ANPR systems are able to check up to 3,000 number plates per hour, per lane, even at speeds of up to 100 mph.[354]

These reads are initially processed locally at each police force's Back Office Facility (BOF), and then they are transferred to the central National ANPR Data Centre (NADC) which ”stores all number plate reads collected by local forces making them available for researching nationally”[355]. The NADC can provide information on vehicle movements that can assist the police in identifying patterns of behaviour of targeted individuals. By 2012 it

[354] UK Motorists, Automatic Number Plate Recognition, 2012. http://www.ukmotorists.com/anpr.asp

[355]ACPO (2013) The police use of Automatic Number Plate Recognition, London, ACPO, p. 8. Available at: http://www.acpo.police.uk/documents/crime/2013/201303CBA-ANPR.pdf

was reported that the National ANPR Data Centre was receiving more than 18 million number plate 'reads' each day[356] and that the database holds details of 11.2 billion vehicle reads.[357] In January 2014, the Guardian reported that there are now more than 8000 cameras in the national ANPR network, which had almost doubled since 2011. These were now recording up to 26 million images a day.[358]

Although ACPO originally wanted, and designed, the system so that the NADC could retain number plate data for five years[359], the current retention period is two years. Some local police forces also have the facility to store the whole image of the vehicle which may include a picture of the driver, although this is often destroyed after 90 days.[360]

As an aid to criminal investigation, it is the intelligence function of ANPR that is most significant. In July 2009, the National Police Improvement Agency (NPIA) and Association of Chief Police Officers (ACPO) issued advice to police forces entitled *Practice Advice on the Management and Use of Automatic Number Plate Recognition* which detailed the extensive data mining potential of the new database.[361] It is now possible for UK police forces to interrogate in excess of 7 billion records per year lodged on the system.[362] The main ways that the data can be exploited through data mining are outlined as:

- vehicle tracking: real time and retrospective;

[356] ibid.

[357] http://www.npia.police.uk/en/docs/NPIA_business_plan_2008-11_final.pdf
[358] ACPO (2005) op. cit., p.14
[359] see http://www.out-law.com/page-9428
[360] ACPO (2013) op. cit., p. 10
[361] http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf
[362] http://www.timesonline.co.uk/tol/news/uk/crime/article7086783.ece. If the National data centre was recording between 10 and 14 million reads per day, that equated to a minimum of 3.6 billion per year and under the DPA this can be held for 2 years.

- vehicle matching: identifying all vehicles that have taken a particular route during a particular time frame;
- geographical matching: identifying all vehicles present in a particular place at a particular time;
- incident analysis: can be used to refute or verify alibi statements, to locate offenders, to identify potential witnesses to specific incidents by identifying vehicles in the location at the time of an incident;
- network analysis: by identifying the drivers of vehicles and their network of associates, ANPR can be used to indicate vehicles that may be travelling in convoy;
- subject profile analysis; by creating an in depth profile of the suspects by integrating information from a variety of data sources such as "crime reports, incidents reports, witness testimony, CCTV, other surveillance, communications analysis, financial analysis, as well as existing intelligence, to define a pattern of behaviour for a subject of interest".[363]

One remarkable aspect of the police national ANPR network is that it is not used to enforce speed restrictions despite the fact that ANPR cameras are ideally suited to calculating the average speed that a vehicle travels between two points on the road network. To understand this, we need to review the contentious history of camera-based speed enforcement in the UK[364]. The 1991 Road Traffic Act allowed, for the first time, evidence collected on camera to be used in the prosecution of motorists for speeding or red light offences. However, throughout the 1990s, camera enforcement remained limited since the 'cost of installing and maintaining speed cameras in the 1990s meant that some police forces had only one in eight devices operating at any one time and drivers were beginning to realise that they were

[363] National Police Improvement Agency (NPIA), (2009*) Practice Advice on the Management and Use of Automatic Number Plate Recognition*, London, NPIA, p. 46.
[364] For and extended discussion of this see: Haines, A. and Wells, H. (2012) Persecution or protection? Understanding the differential public response to two road-based surveillance systems *Criminology and Criminal Justice* 2012 12: 257

unlikely to be caught.'[365] In 2000, the government sponsored a pilot Safety Camera Programme, which allowed for the income derived from fines to be retained in eight pilot areas and to be used pay for the costs of enforcement and other road safety activities. In 2001, legislation was introduced that allowed the system to be rolled out nationally.[366] The effect was a dramatic rise in the number of enforcement cameras: from 1,935 in England and Wales in 2000 to 5,562 by 2006[367] and, by 2009, the number had increased to around 6,000.[368] Correspondingly, the number of prosecutions and fixed penalty notices arising from camera-based enforcement of speeding and red light infractions increased eight fold between 1995 and 2005, to a total of just over 2 million.[369]

As a consequence, the surveillance of motorists for the purposes of enforcing road traffic law has been one of the most politically contentious surveillance measures, with national newspapers,[370] opposition ministers,[371] and pressure groups[372] accusing the government of trying to criminalise the motorist,[373] exaggerating the beneficial effects of speed cameras and generating a stealth tax through the collection of fines.[374] In the run up to the 2010 general election, the shadow transport secretary, Theresa Villiers, declared at the annual Conservative Party conference:

---

[365] Louise Butcher, (2009) 'Roads: Speed Cameras', *House of Commons Briefing Paper*, Standard Note:

London, House of Commons Library, p. 5.

[366] http://www.dft.gov.uk/pgr/roadsafety/speedmanagement/nscp/nscp/thenationalsafetycameraprogr4597

[367] http://www.independent.co.uk/news/uk/politics/tories-put-brake-on-growth-in-speed-cameras-1798181.html

[368] http://www.speedcamerasuk.com/speed-camera-faqs.htm

[369] http://www.dft.gov.uk/adobepdf/162469/221412/217792/4212241/transportstatisticgreatbrit. and http://www.justice.gov.uk/publications/docs/motoring-offences-and-breath-stats-2006-ii.pdf

[370] http://www.dailymail.co.uk/news/article-1177303/Milking-motorist-How-speed-cameras-rake-10-000-HOUR-drivers.html

[371] Located at http://www.epolitix.com/latestnews/article-detail/newsarticle/theresa-villiers-speech-on-ending-the-expansion-of-fixed-speed-cameras/

[372] See, for example, http://www.taxpayersalliance.com/TPAmanifesto.pdf and http://www.safespeed.org.uk/

[373] http://news.bbc.co.uk/1/hi/uk_politics/7854774.stm

[374] see http://www.dailymail.co.uk/news/article-1177303/Milking-motorist-How-speed-cameras-rake-10-000-HOUR-drivers.html

> "It's time to put a stop to Labour's cash cow camera culture. Ladies and gentlemen, a Conservative government would not fund any *new* fixed speed cameras because they are not the best way to make our roads safer."[375]

The legitimacy of the National ANPR system has been promulgated by a strategic decision to promote it as not being concerned with enforcing speed restrictions. The proliferation of speed enforcement cameras has been one surveillance practice that has led to sustained opposition and resistance[376] and, to ensure that the development of the National ANPR system did not arouse similar opposition, police forces have been keen to distance the National ANPR system from speed enforcement. As one police force typically declares:

> "ANPR cameras are not used in Northern Ireland to catch speeding or otherwise law-abiding motorists. ANPR cameras are not used to generate money for the government or other agencies."[377]

In the UK there have been no formal and methodologically adequate evaluation studies of the effectiveness of ANPR as a crime. The PA consultancy evaluation of the UK pilot scheme concluded that it had been very successful; however, their criteria of success was the increase of the arrest rate per officer, rather than whether the system led to a reduction in the crime rate or an increase in detections. It is perhaps surprising given the centrality of ANPR to national policing strategy, that no formal evaluation has been conducted in the ten years since the pilot study. And, while in their most recent briefing document on ANPR, ACPO writes, the "police believe access to the information provided by ANPR enables them

[375] Cited at http://www.thenewspaper.com/news/29/2922.asp
[376] Haines and Wells (2012) op. cit.
[377] http://www.psni.police.uk/index/updates/anpr-cameras.htm

to identify suspected offenders and vulnerable people more efficiently",[378] they provide no evidence to support this claim.

5. Four public controversies surrounding the operation ANPR in the UK

5.1 ANPR and the Surveillance of Domestic Extremists

The surveillance of political activists and protesters has long been a function of the British police. In 1882 a 'special branch' was formed as part of the Metropolitan Police after a spate of Fenian bombings in London and, while the surveillance of the Irish republican movement remained the central remit of Special Branch for almost the next hundred years, its mission was extended to include anarchists, communists, peace campaigners and trade unionists, to name but a few.[379]

The most recent incarnation of the surveillance of activists and protesters has been carried out by the National Domestic Extremist Unit, which was directed by the ACPO Sub-Committee on Terrorism and Allied Matters. In the wake of a number of scandals, in 2011, the management of domestic extremism units was moved from ACPO to the Counter Terrorism Unit of the Metropolitan police, which is now responsible for the National Public Order Intelligence Unit (NPOIU).[380]

NPOIU runs the database of 'domestic extremists' which collates intelligence supplied by police forces across England and Wales and deploys its own surveillance teams at demonstrations and sites of political protests.

[378] ACPO (2013) op. cit., p. 11
[379] Bunyan, T. (1977) The History and Practice of The Political Police in Britain, London Quartet Books,
[380] http://www.acpo.police.uk/NationalPolicing/NDEDIU/AboutNDEDIU.aspx

The ACPO definition of domestic extremism is as follows:

> "Domestic extremism and extremists are the terms used for activity, individuals or campaign groups that carry out criminal acts of direct action in furtherance of what is typically a single issue campaign. They usually seek to prevent something from happening or to change legislation or domestic policy, but attempt to do so outside of the normal democratic process."[381]

The operational enactment of this concept has been criticised in a recent Her Majesty's Inspectorate of Constabulary review as being far too wide ranging.[382] In particular there have been allegations that almost anyone attending a political protest may be subject to intimidating surveillance tactics which include "following, stop and searching and, photographing peaceful protestors by Forward Intelligence Teams".[383] [384] In June 2013, it was reported that 8,931 individuals had a record on the Domestic Extremist database and that, "Senior officers familiar with the workings of the unit have indicated to the Guardian that many of the campaigners listed on the database have no criminal record."[385]

While the activities of the Police Forward Intelligence Units has come under scrutiny, it is clear, however, that ANPR data is being used to routinely track and monitor political protestors and then to log them on the 'domestic extremists' database, and that inclusion on the database is not confined to those who perpetrate violence and disorder. Merely being "associated" with protests that have given rise to "crime, disorder and the deployment of

[381] the ACPO definition is cited at page 11 of http://www.hmic.gov.uk/media/review-of-national-police-units-which-provide-intelligence-on-criminality-associated-with-protest-20120202.pdf
[382] ibid.
[383] http://www.fitwatch.org.uk/fit/
[384] The Guardian Newspaper "Are you a 'Domestic Extremist'? http://www.theguardian.com/uk/2011/apr/11/domestic-extremist-police-databases
[385] http://www.theguardian.com/uk/2013/jun/25/undercover-police-domestic-extremism-unit

significant resources", appears to give the police sufficient justification to include a person on the database and subject them to extensive tracking and repeated stops.[386] But even those attending peaceful protests have also been logged. As the Guardian newspaper revealed, a man with: “no criminal record, was stopped more than 25 times in less than three years after a 'protest' marker was placed against his car after he attended a small protest against duck and pheasant shooting”.[387] Similarly, John Catt, an eighty-five year old peace campaigner and his fifty year old daughter had their presence recorded at over 80 lawful demonstrations over a period of four years. As well as information gained by Forward Intelligence Teams, Mr. Catt's movements were also being recorded on the emergent National ANPR Network. In July 2005, he and his daughter:

> “were stopped by police under the Terrorism Act after driving into east London to help a family member move house. They later discovered police had placed a marker against their car registration on the database, triggering an alert – "of interest to public order unit, Sussex police" – each time they drove beneath an automatic number plate reading camera.”[388]

In 2009, Fitwatch reported that ANPR units were being used to monitor and intercept climate change activists’ cars during the protests around the Kingsnorth Power station. However much of the police activity was declared unlawful when three activists were awarded compensation from the Kent Police who admitted “they had been unlawfully stopped and searched”. [389]

5.2 The Guardian versus Devon and Cornwall police: Can we know the location of the cameras?

[386] http://www.guardian.co.uk/uk/2009/oct/25/surveillance-police-number-plate-recognition
[387] http://www.guardian.co.uk/uk/2009/oct/25/police-domestic-extremists-database
[388] http://www.theguardian.com/uk/2010/jun/25/peace-campaigner-classified-domestic-extremist
[389] http://www.theguardian.com/environment/2010/jun/14/police-compensation-kingsnorth-climate-protesters

In July 2009 Mr. Mathieson of the Guardian Newspaper filed a Freedom of Information (FOI) request on behalf of the Guardian asking for the locations of the ANPR cameras used by the Devon and Cornwall Police. The Devon and Cornwall Police refused, relying on exceptions under the FOI Act (2000) in relation to the prevention, detection, and prosecution of offenders, the administration of justice and national security.[390]

On the 22nd of September 2009 he appealed to the Information Commissioner's Office (ICO). It took the ICO precisely one year and a day to reach its judgement. The ICO said that Devon and Cornwall Police were correct in refusing to provide the locations of automatic number-plate recognition cameras although it accepted that the extent of the ANPR network "is of considerable significance to the balance of the public interest". [391] However, the public interest in disclosing the locations of the cameras has to be balanced against the public interest in the police not revealing the location of the cameras in order to prevent crime and apprehend offenders. Although the two public interest arguments were "finely balanced" with "very significant weight both for and against disclosure",[392] the ICO ruled against disclosure. The Guardian appealed that decision to the First Tier Information Rights Tribunal in December 2010. In April 2011, Judge Alison McKenna ruled "that the public interest in disclosure outweighs the public interest in maintaining the exemptions in the circumstances" and ordered that the ICO decision be put aside and the Police disclose the location of the cameras within 35 days. Of particular note was that the Tribunal argued that the ICO:

[390] http://www.theguardian.com/commentisfree/libertycentral/2011/may/17/automatic-numberplate-recognition-cameras-anpr
[391] Reference: FS50270424,Freedom of Information Act 2000 (Section 50),Decision Notice, Reference: FS50270424, Date: 23 September 2010, page 7.Available at: http://ico.org.uk/~/media/documents/decisionnotices/2010/FS_50270424.ashx page 7.
[392] ibid., p. 8.

> "did not fully consider the impact of the DPA and the rights of access to information captured by the ANPR cameras which (it appears to have been accepted by others, including ACPO) constitutes personal data. It is clearly difficult for members of the public to exercise their rights in relation to the DPA if they cannot know where the cameras are located."[393]

Furthermore the tribunal noted that the evidence produced by the Devon and Cornwall Police as to the effectiveness of ANPR cameras was "weak" and not strong enough to tip the balance against public disclosure in a matter of considerable national importance.[394]

Devon and Cornwall Police immediately appealed this ruling to the Upper Tribunal on the grounds that the First Tier Tribunal had not properly considered the exemptions under section 31 of the FOI Act regarding the necessity of non-disclosure for the purpose of the detection and prevention of crime but, more importantly, it had failed to consider at all the exemptions under section 24, in relation to National Security.[395] The judge of the Upper Tier Tribunal agreed that section 24 had not been considered but ruled that, rather than make a decision himself, the case should be referred back to a newly constituted First Tier Tribunal which could consider the case afresh, with due regard to the national security exemption.

On the 18th of June 2012, the First Tier Tribunal unanimously decided to dismiss Mr Mathieson's appeal. It is noteworthy that the form of the judgment makes it impossible to determine the relative weight applied to each of the grounds for exemption, but it seems likely that National Security was the trump card since it was argued: "we are bound also to take account of the fact, although the risk may have been small, if disclosure of the

[393] Appeal No. EA/2010/0174, heard before Alison McKenna, Tribunal Judge In the First-Tier Tribunal General Regulatory Chamber (Information Rights) 11 April 2011, page 11
[394] ibid.
[395] Case No. GIA/1554/2011 The Upper Tribunal, Administrative Appeals Chamber

information requested meant, for example that a terrorist incident took place which might otherwise have been avoided, the results would be catastrophic."[396] [397]

5.3 Royston's 'Ring of Steel' and the legality of the ANPR

On 7th June 2011, three privacy rights groups, 'Big Brother Watch'[398], 'No CCTV'[399] and 'Privacy International',[400] made a formal complaint to the Information Commissioner that the ANPR surveillance around the town of Royston was operating unlawfully.[401] Royston is a small town in Hertfordshire, with a population of 15,000 people, which sits on a convergence of east and west routes between the major national roads of the A11, the M11 and the A1M.[402] Hertfordshire Constabulary as part of the National ANPR network had installed 7 cameras on all the approach roads in and out of the town, which effectively meant that "no vehicle could enter or leave Royston without being recorded on camera".[403]

The complaint made five substantive arguments:

First, that it was extraordinary that such an extensive surveillance network could be constructed "without the result of any Parliamentary debate, Act of Parliament or even a Statutory Instrument", and more extraordinary given that the strategy was implemented and run by ACPO, a private limited company, which was unaccountable to parliament.[404]

Second, that the system breached the second principle of the Data Protection Act (DPA)1998 which states that "personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that

---

[396] Appeal No. EA/2010/0174, heard before HH Judge Shanks In the First-Tier Tribunal General Regulatory Chamber (Information Rights) 18 June 2012, page 7
[397] Appeal No. EA/2010/0174, heard before Alison McKenna, Tribunal Judge In the First-Tier Tribunal General Regulatory Chamber (Information Rights) 11 April 2011
[398] http://www.bigbrotherwatch.org.uk/
[399] http://www.no-cctv.org.uk/
[400] https://www.privacyinternational.org/
[401] http://www.no-cctv.org.uk/materials/docs/Royston_Ring_of_Steel_ANPR_Complaint.pdf
[402] http://www.theguardian.com/uk/2011/jul/28/royston-under-surveillance-police-cameras
[403] http://www.north-herts.gov.uk/aksnherts/users/public/admin/kab12.pl?cmte=RAD&meet=2&arc=20
[404] Complaint by NO CCTV, Privacy International, and Big Brother Watch to the Information Commissioner, with regard to 'Royston ANPR Ring of Steel', the full text of the complaint is available at: http://www.no-cctv.org.uk/materials/docs/Royston_Ring_of_Steel_ANPR_Complaint.pdf, page 7

purpose"[405] Their objection rests on the basis that the justification put forward by Hertfordshire Constabulary was:

> "vague at best and furthermore it seems that Hertfordshire Constabulary along with other forces believe that they can simply state objectives without any evidence that the objectives are attainable. This is an absurdity. The fact that the stated purposes of ANPR are not backed up by evidence that they are attainable must surely further undermine Hertfordshire Constabulary's compliance with principle two of the Act."[406]

Third, that the system was in breach of the fifth principle of the Data Protection Act which states: "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes". The complainants argued that Hertfordshire Constabulary appeared to be keeping data for longer than the legally proscribed period of two years, and that even this retention period was excessive.[407]

Fourth, that the first data protection principle that data should be processed fairly and lawfully requires that "part of fair processing is the requirement to notify people that they are being filmed".[408] The absence of signage in the Royston system makes it in breach of the fair processing requirement.

Fifth, that under the DPA, for data processing to be lawful, it must be 'necessary' and 'proportionate' and that such an extensive blanket surveillance is neither. As they argue:

> "In the past totalitarian regimes instituted road blocks to check citizens' papers at a series of internal borders. The police use of ANPR as a mass surveillance tool to record the movements of all cars and the justification given by Hertfordshire Constabulary for a ring of cameras around Royston such that "no vehicle could enter or leave Royston without being recorded by a camera" because the town is in "a

[405]ibid., p. 4
[406]ibid., p. 7
[407]ibid., p. 9
[408]ibid., p. 10

> location of importance on the borders of Hertfordshire and Cambridgeshire" is surely equivalent to an automated checkpoint system that cannot be necessary in a democratic society to meet any of the purposes set out by Hertfordshire Constabulary."[409]

It took the ICO two years and one month to rule on the complaint. On the 15th July 2013, the ICO issued an enforcement notice against the Chief Constable of Hertfordshire Constabulary requiring that the data controller:[410]

> "Refrain from processing personal data… except to the extent that such can be justified to the satisfaction of the Commissioner as being in compliance with the First and Third Data Protection Principles following the conduct of a Privacy Impact Assessment or similar impact assessment that defines the pressing social need, assesses the likely effectiveness of the proposed measures in addressing this, identifies the likely impact on the private life of individuals and determines that the proposed measures are a proportionate interference after taking into account any additional safeguards that might be provided."[411]

Hertfordshire Constabulary duly conducted a Privacy Impact Assessment and removed an unspecified number of cameras. Subsequently, the ICO declared itself to be happy as to the proportionality of the scheme.[412]

The ruling did not satisfy the complainants. In their view it represented a hollow victory because the ICO had "side stepped" the real issue by reducing the complaint to a balancing of the ECHR article 8 right to privacy against the State's right to qualify it for particular purposes. In effect the ruling merely asked the police to state the reasons for the

[409]ibid., p. 12
[410]http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf
[411] ibid., p. 3
[412] See, http://ico.msgfocus.com/q/1AFzluAAMi/wv#story10

qualification of the right, thereby reducing the "whole issue… to a meaningless box ticking exercise." [413]

5.4 Project Champion: The intensive surveillance of an ethnic minority community

Project Champion was a scheme to encircle two, predominately Asian, residential communities in Birmingham - Sparkhill and Washwood Heath - with overt and covert CCTV and ANPR cameras. In was initiated in late 2007 by the West Midland Counter Terrorism Unit (WTU) in the context of a heightened security threat following the discovery of an unexploded car bomb in London, and a terrorist attack on Glasgow Airport.[414] More specifically, earlier in 2007:

> "West Midlands Police had thwarted a plot to kidnap and behead a Muslim soldier. The investigation, known as Operation Gamble, was focussed on a number of mostly British-born Pakistani men living in Birmingham. The investigation was centred on the areas of Alum Rock and Sparkhill."[415]

The areas of Alum Rock and Sparkhill sit in the Washwood Heath and Sparksbrook districts of Birmingham. According to the 2001 population census, 27,822 people were resident in the 5.2 square kilometres of Washwood Heath ward, 57% of whom were described as coming from the ethnic minority population.[416] Sparkbrook has a population of 31,485, over 70%

[413] ICO ruling replaces "Ring of Steel" with Mass Surveillance Roulette - 7/3/14 - available at: http://www.no-cctv.org.uk/press.asp
[414] Thornton, S. (2010) *Project Champion Review: An independent review of the commissioning, direction, control and oversight of Project Champion; including the information given to, and the involvement of, the community in this project from the initiation of the scheme up to 4 July 2010*; Thames Valley Police.
[415] ibid.; see also "Man admits plot to behead soldier", *BBC News*. 2008-01-29. http://news.bbc.co.uk/1/hi/uk/7215081.stm
[416] see: http://www.birmingham.gov.uk/washwoodheath

belonging to ethnic minority communities, in an area of 3.91 Kilometres.[417] In total the project consisted of 216 surveillance cameras covering the two districts, 46 CCTV cameras, 8 of which were covert, and 170 dedicated ANPR cameras, 64 of which were covert.[418]

The rationale for the scheme was outlined in the business case made on behalf of West Midland Counter Terrorism Unit to the ACPO Terrorism and Allied Matters (TAM) sub group. It stated:

> "The UK is currently facing the most serious and sustained threat from international terrorism ever known. The threat remains real (Security Level: Severe). The events in London of 2005 demonstrated the need for all agencies to enhance their own capacity and capability; working together requires capability to operate across organisational and geographic boundaries. The West Midlands area contains significant features of vulnerability.[419]
>
> (Next paragraph is redacted)
>
> The opportunity to capture data 24/7 instead of an "as and when" basis represents a step change. Deployment decisions based on an absence of knowledge or decisions based on assessments of risk (which may or may not be complete) concerning safety of personnel and the real and potential risks of operational compromise arising from

[417] see: http://www.birmingham.gov.uk/Sparkbrook
[418] Birmingham City Council (BCC) (2010*) Project Champion: Scrutiny Review into ANPR and CCTV Cameras*, Birmingham City Council, 02 November 2010, page 7.

traditional methods, are all drivers for developing the “stand off” options that Project Champion has been developed to deliver.”[420]

It outlined the core vision as:

> “Creating a ‘net’ of ANPR to capture target vehicle movements of subjects entering, leaving or within two distinct geographical areas within the city of Birmingham.”

And:

> “Delivering an infrastructure for data capture and retention that will add value locally in respect of current operations in the short, medium and long term and available for analytical use in current and future operations on a local, regional and national level.” [421]

On the basis of this case, which also suggested that financial support would be forthcoming from Birmingham City Council, ACPO agreed to fund the scheme to the value of 3 million pounds. Because of the sensitivity of the proposals, it was agreed the project should be conducted on a 'need to know' basis and, according to the minutes, this was backed up by more formal actions:

> “The project had insisted on SC [security check] clearance for the Project Manager/ Bid Team and minimum vetting process for contractors. Indoctrination of personnel

[420] ACPO Strategic Outline Business Case - ACPO TAM Business Area, available at: https://www.whatdotheyknow.com/request/36626/response/117902/attach/3/Disclosed%20information%20West%20Mids%20Business%20Case.pdf, page 3.
[421] ibid., p. 3

has also taken place, together with signing the Official Secrets Act, copying of documents will not be permitted."[422]

Had the scheme limited itself to a covert operation run by the West Midlands Counter Terrorism Unit, it is unlikely that we would have ever known about its existence. However, since the scheme's success seems to have been predicated on a blanket coverage of all vehicle movements, with additional CCTV images of drivers and pedestrians, along dozens of streets, the sheer number of cameras and the infrastructure required to support them could not have been put in place covertly. It was therefore decided to 'piggy-back' the scheme on an expansion of the already existing overt CCTV scheme in the neighbourhood, and market it as a solution to the existing crime problem in the area. As a result:

"the involvement of the CTU took a back seat and the Project moved forwards as a Safer Birmingham Partnership crime reduction / community safety initiative. CTU insignia were replaced by the Safer Birmingham Partnership (SBP) logos and an 'open document' was produced as a brief on Project Champion."[423]

The 'open document', which was widely circulated in the community and used as a briefing document for local councillors, stressed that the scheme was overseen by the Safer Birmingham Partnerships, and that the cameras would specifically address serious acquisitive crime, serious violent crime, violent extremism, and anti social behaviour. It went on to state that it had been funded by the Home Office, and to pose the question:

"Has this anything to do with preventing acts of terrorism?"

[422] BCC 2010 op. cit., p. 33.
[423] Thornton, S (2010) op. cit., p. 17.

To which it gave the answer:

> "This is not the focus of the operation. The cameras will be utilised to tackle all types of crime to help keep our communities as safe as possible."[424]

This was reiterated by The Assistant Chief Constable at a meeting with local councillors, the minutes of which record:

> "ACC Hyde responded that if he said that additional CCTV and ANPR facilities would not have any benefit around Counter Terrorism then he would be lying and that is why this element was including [sic] in the briefing note however the reassurance and crime prevention benefits are far greater."[425]

The problem, of course, with all these statements is that they were simply untrue. The scheme was first and foremost a counter terrorism scheme, funded by ACPO, not the Home Office, under their Terrorism and Allied Matters Sub-committee, and implemented by the West Midlands Counter Terrorism Unit.

As Thornton's review concluded:

[424] Councillors Briefing note produced by The Safer Birmingham Partnership available at https://www.whatdotheyknow.com/.../Cllrs%20Briefing%2022.1.10.doc
[425] BCC (2009) op. cit., p. 3.

> "When the cameras went live at the completion of Project Champion (scheduled for May or June 2010) there would have been no local facility to view the cameras and nobody in place to monitor them."[426]

Indeed, from the outset, the implementation team had agreed that:

> "In consultation with WM CTU it has been agreed that the Champion system will remain independent of the existing Local Authority CCTV environment with the possible exception of sharing power supplies and the mounting of CCTV cameras on existing Council CCTV poles. In these instances, the CCTV cameras will operate over the WM CTU transmission solution."[427]

And:

> "It is understood that the CCTV images captured by the Champion CCTV system are not going to be accessible to partners such as Birmingham City Council as such access could result in an operation becoming compromised."[428]

In January 2010, work began on installing the cameras, which involved digging up the roads and pavements to install the cabling and to erect the 'supersized lamp-posts' necessary to hold the cameras. By April 2010, as local residents became aware of the size of the scheme, opposition started to mobilise[429] and, in May, the project risk register was updated to note that:

[426] Thornton (2010) op. cit., p. 30.
[427] ibid. pp. 15-16
[428] ibid. pp. 21-22
[429] see; http://spyonbirmingham.blogspot.co.uk/

> Following the installation of the CCTV poles public and political reaction and pressure has become pronounced. This pressure includes calls for poles to be removed or relocated for numerous reasons, including big brother concerns and aesthetics.[430]

On the 4th June 2010, the story broke in the leading national newspaper, The Guardian, under the headline 'Surveillance Cameras in Birmingham Track Muslims' Every Move'[431]. As a result of the mounting pubic disquiet and community anger, on the 16th of June, the Assistant Chief Constable of West Midland Police and The Safer Birmingham Partnership announced that the work on the scheme would be halted and the cameras covered by plastic bags.[432]

Two inquiries were set up to investigate the issues, the first was commissioned by The West Midlands Police to be conducted by Sarah Thornton the Chief Constable of Thames Valley Police,[433] but also a member of ACPOs Terrorism and Allied Matters sub-committee, which funded the original scheme. The second was by Birmingham City Council.[434]

The Birmingham City Council report concluded that Project Champion was "unacceptable in the way it was constructed to target the Muslim community"; that the police had engaged in a tactic to "deliberately mislead Councillors"; [435] and "there was a catastrophic lack of

[430] Thornton 2010 op. cit., p. 27
[431] http://www.theguardian.com/uk/2010/jun/04/surveillance-cameras-birmingham-muslims
[432] "'Plastic bags to be put over Birmingham 'terror cameras'" available at: http://www.bbc.co.uk/news/10337961
[433] Project Champion Review; An independent review of the commissioning, direction, control and oversight of Project Champion; including the information given to, and the involvement of, the community in this project from the initiation of the scheme up to 4 July 2010.
[434] Birmingham City Council (BCC) (2010) Project Champion: Scrutiny Review into ANPR and CCTV Cameras, Birmingham City Council, 02 November 2010
[435] ibid. p. 58

inquisitiveness" from the Police Authority and the Safer Birmingham Partnership both tasked with scrutinising the Project on the public's behalf.[436]

The police enquiry[437] concluded that "from the start questions should have been asked about its proportionality, legitimacy, authority and necessity; and about the ethical values that underpinned the proposal'"[438] Moreover, the report found that the affair had resulted in "significant community anger and loss of trust".[439] And perhaps most importantly, the Chief Constable concluded: "I found little evidence of thought being given to compliance with the legal or regulatory framework". [440]

While some saw this as a damning indictment of police practices,[441] what has never been addressed is the role that ACPO's Terrorism and Allied Matters subcommittee had in funding, planning and authorising the scheme. In both enquiries an examination of their role is absent.

6. Surveillance and democracy

On the one hand, we can view the conclusion of the Project Champion case as a victory for democracy. Concerned citizens mobilized, exercising their right of free association and freedom of expression to garner public opposition to the scheme. Locally elected politicians raised issues of concern with the local council and police. The issues gained national

[436] ibid. p.60
[437] Project Champion Review; An independent review of the commissioning, direction, control and oversight of Project Champion; including the information given to, and the involvement of, the community in this project from the initiation of the scheme up to 4 July 2010.
[438] ibid. p.48
[439] ibid. p.47
[440] ibid. p.38
[441] See: http://www.no-cctv.org.uk/docs/Whats%20Wrong%20With%20ANPR-No%20CCTV%20Report.pdf

prominence when the 'free' press reported it and the issue was brought to the attention of the House of Commons. The police apologised, the system was abandoned and, in the end, most of the cameras were removed.

However, on closer inspection, Project Champion and the other controversies we have outlined reveal the weakness of the Rule of Law. The Rule of Law implies that the powers that are exercised by individuals or organisation have been deemed appropriate by a legislative body and that the exercise of that power can be reviewed by the courts and the legislative assembly to ensure that it is appropriate and not excessive. In democratic states, there is an assumption that the legislative body will be elected, whereby office-holders justify their claim to continue in office by subjecting their record of performance to the scrutiny and approval of the electorate. This requires both transparency and accountability. Transparency is necessary so that the electorate may scrutinise the activities of government, and accountability is the mechanism by which power is held to account.

7. The Rule of Law

The first question we need to ask then is by what law do the police have the power to install ANPR cameras to undertake mass surveillance of the citizenry and to create a centralised database of vehicle movements across the country, which then can be subject to extensive data mining procedures to build up profiles of individual movements and associations? The answer to the question is none. This was confirmed by the ACPO's rather terse response to a recent FOI request which stated:

> "The use of ANPR merely provides information on which officers may act. It does not require any legislation or statutory powers."[442]

Even so, given that individual police forces provide the details of vehicle movements to a central police data warehouse established at Hendon for storage and analysis, we could ask, under what law do the police centralise the data? Like with general open street CCTV, there is no law that expressly gives them this right to record and store images and information derived from them. However, because a car number-plate, like a picture of a person, may be considered personal data, the data is subject to the provision of the Data Protection Act. And although the Act does expressly give them the right to store ANPR data, it does limit the length of time that it can be retained and creates the legal basis upon which information can be processed and shared.[443]

If there is no specific law governing the installation or recordings of ANPR cameras but merely permissive legislation which limits its retention and enables the data captured to be moved between police forces, we could then ask, is there a law governing their use?

Here we find that there is. Where a camera is covert and the purpose of its operation is to target specific individuals, then it constitutes 'directed surveillance' under the provision of the Regulation of Investigatory Powers Act 2000 (RIPA). This requires high level and special authorisation and reporting to the Office of Surveillance Commissioner, whose job it is to oversee covert surveillance. As various FOI requests have found, for operational reasons, the police are not prepared to identify the sites of ANPR operation, neither do they generally

[442] Details of statutory powers relating to ANPR made by Marie Koenigsberger under the Freedom of Information request to ACPO on the 4th September 2009. Avialable at: https://www.whatdotheyknow.com/request/details_of_statutory_powers_rela?unfold=1

[443] National Police Improvement Agency (NPIA) (2011) Memorandum of Understanding to support the submission and access to data held on the National ANPR Data Centre (NADC)

warn motorists that an area is under ANPR Surveillance and some cameras are, indeed, really 'covert'. Given that the positioning of ANPR cameras is deemed secret, then the issue arises as to whether they constitute a covert surveillance device. For covert surveillance to be legal it needs to have an express legal basis, but there is no statutory basis for the operation of ANPR, as widespread usage was not considered when the Regulation of Investigatory Powers Act was introduced.

It would seem that the law that does, in some circumstances, regulate the use of ANPR, but this is being sidestepped by the police. They appear to be routinely using the ANPR database to carry out directed surveillance without RIPA authorization. So much so that the Surveillance Commissioner accused them of deliberately circumventing the law.[444] This lack of attention to their legal obligations was also noted by the Thornton review of Project Champion, which concluded:

> "There was, however, nothing available to the Review Team that demonstrated that the authorisation process for the use of the cameras had been considered, and there was no policy, plan, or procedures in place for their management in compliance with RIPA or other applicable legislation, codes, or guidance."[445]

8. *Governance - the democratic deficit*

Surveillance is a legitimate element of democratic systems. However, the fundamental difference between dictatorial and democratic systems, with regard to surveillance, lies in its accountability: while in a dictatorial system, state surveillance cannot be overseen and

[444] Page 18 http://www.statewatch.org/news/2012/jul/uk-surveillance-commissioner-report-2011-2012.pdf
[445] Thornton, S (2010) p17Project

controlled by the citizens, at least in an institutionalized form, in democracies there should be institutions and mechanisms established for this purpose.

The creation of a national database of all citizens' vehicle movements would seem to warrant an explicit legislative basis and clear mechanisms for accountability and governance, not least to ensure that privacy, data protection, and human rights concerns are properly addressed. This is not the case. There is no statutory authority for the creation of the national ANPR database, its creation was never agreed by parliament, and no report on its operation has even been laid before parliament. Rather it is the creation of ACPO.

ACPO has been responsible for developing the National ANPR strategy, monitoring its implementation and developing the local and national systems to store, collate and analyse vast amounts of personal data. ACPO is, however, a non-statutory body, a private limited company which, although engaged in developing and implementing national policy in relation to policing, is not accountable to parliament, the home secretary or any other body for its activities. Nor was it subject to FOI requests, during the development of the National ANPR infrastructure since it was exempt as a limited company.[446] While ACPO owns the National Data Centre which houses the National ANPR Database it does not own the data that it collates and nor is it responsible for its integrity. The data is owned by the individual police forces who collect and download it to the National Database, and it is the individual Chief Constables who are responsible for its accuracy and for ensuring compliance with the Data Protection Act.

As Her Majesty's Inspectorate of Constabulary (HMIC) has identified, in the context of a review of public order policing, there is considerable lack of transparency and uncertainty

[446] However since November 2011 this has changed and they are now subject to FOI requests, see http://www.acpo.police.uk/FreedomofInformation/ACPOpublicationsFoI.aspx

about ACPO's role, "particularly when it is engaged in quasi-operational roles, such as the collation and retention of personal data",[447]and that its governance and accountability structures need to be made fit for purpose. As they go on to argue:

> "HMIC considers that ACPO's co-ordinating role and operational support function for the police service should be formally recognised. (...) However, ACPO's current undefined locus is no longer sustainable and there are significant questions to address regarding the status and accountability of ACPO's quasi-operational units such as NPOIU[448], NETCU[449] and NDET[450] which perform significant intelligence functions, including commissioning, gathering and analysing intelligence and collating and retaining personal data."[451]

Moreover serious consideration needs to be given to the formal status of ACPO and whether it should be constituted as a:

> "statutory public body, centrally funded by and accountable to Government and tasked with providing a coordinating role and operational support function for the police service at the national level. ACPO would retain responsibility for its current quasi-operational units but as a public body, would be required to comply with (among others) the Data Protection Act 1998, the Human Rights Act 1998 and the Freedom of Information Act 2000."[452]

---

[447] Her Majesty's Inspectorate of Constabulary (HMIC) (2009) *Adapting to Protest – Nurturing the British Model of Policing,* London, HMIC page 150.
[448]National Public Order Intelligence Unit
[449] National Extremism and Tactical Coordination Unit
[450] National Domestic Extremism Team
[451] Her Majesty's Inspectorate of Constabulary (HMIC) (2009) *Adapting to Protest – Nurturing the British Model of Policing,* London, HMIC page 150.
[452] ibid., p. 151

The lacunae in governance surrounding ANPR, has been highlighted in the political debate over surveillance over the last decade with calls for increased regulation of the surveillance activities of the state gaining momentum in the run up to the 2010 general election. We will briefly conclude this case study with an overview of the political response and the fate of ANPR legislation.

In 2006, the UK Information Commissioner asked the *Surveillance Studies Network* [453]to produce a report on the so-called 'Surveillance Society'. The report highlighted, amongst many other things, the creation of the National ANPR network and the general problem of governance of the emergent surveillance infrastructure. The report attracted widespread national publicity.[454]

In March 2007 the *Home Affairs Committee* launched a wide-ranging enquiry into the growth of public and private databases including the use of ANPR. Their final report *A Surveillance Society?,* published in 2008, included a raft of recommendations.[455] In 2007, the *House of Lords Select Committee on the Constitution* also launched an enquiry entitled *Surveillance: Citizen and the State* with the final report being published in 2009.[456] The report called for the statutory regulation of CCTV (and by default ANPR) and particularly highlighted the issue of the lack of consent in relation to the collection of ANPR data. In September 2009, in the run up to the general election, Dominic Grieve, then shadow justice minister, launched a Conservative Party Policy Paper entitled *Reversing the Rise of the Surveillance State*.[457] Although the use of ANPR is not explicitly mentioned, the general issue of the lack of regulation of the State's growing number of database is a key issue for the report. The

---

[453] Ball, K., Lyon, D., Murakimi-Wood, D., Norris C. and Raab, C. *A Report on the Surveillance Society for the Information Commissioners office by the Surveillance Studies Network: Full Report.* pp 1-102.
Available at:
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

[454] see for instance: *BBC* http://news.bbc.co.uk/1/hi/uk/6108496.stm

[455] *A Surveillance Society?* Fifth Report of Session 2007–08 Volume I HC 58-I

[456] House of Lords, (2009) *Surveillance: Citizens and the State* Volume I: HL Paper 18–I London : The Stationery Office.

[457] Grieve, D. & Laing, E. MP, (2010) *Reversing the Rise of the Surveillance State*, London, Conservative Party

Liberal Democrat manifesto also declared “decades of Labour and Conservative rule have overthrown some of the basic principles of British justice and turned Britain into a surveillance state” and in particular promised to introduce statutory regulation of CCTV surveillance.[458]The Conservative Party Manifesto declared:

> Labour have subjected Britain’s historic freedoms to unprecedented attack. They have trampled on liberties and, in their place, compiled huge databases to track the activities of millions of perfectly innocent people, giving public bodies extraordinary powers to intervene in the way we live our lives.[459]

The need for statutory regulation was also recognised at the inception of the National ANPR network when, in 2004, the Home Secretary David Blunkett declared “it is likely to lead to ANPR enabling legislation as soon as parliamentary time allows”.[460] In 2007, the Chief Surveillance Commissioner called for statutory regulation and in 2010 in the wake of the Project Champion controversy, the then home secretary Teresa May was reported as ordering that the national ANPR network be placed under statutory footing.[461]

In February 2011, the coalition government launched the *Protection of Freedoms Bill*. However, rather than placing CCTV and ANPR under a statutory footing it proffers a new regulator, the Surveillance Camera Commissioner, whose sole role 'is to encourage compliance with the surveillance camera code of practice'[462]. Under the ironic banner of “surveillance by consent[463]” the Home Office declared that "consent is at the heart of the

---

[458] Liberal Democrat Manifesto for the 2010 general election. Page 93. Avialable at http://www.astrid-online.it/Dossier--R3/Documenti/Elezioni 2/libdem_manifesto_2010.pdf
[459] Conservative Party Manifesto for the 2010 general election, page 79. Available at: http://media.conservatives.s3.amazonaws.com/manifesto/cpmanifesto2010_lowres.pdf
[460] Preface to Denying Criminal the Use of the Roads available at http://www.popcenter.org/problems/residential_car_theft/PDFs/Henderson.pdf
[461] http://www.theguardian.com/uk/2010/jul/04/anpr-surveillance-numberplate-recognition
[462] https://www.gov.uk/government/organisations/surveillance-camera-commissioner
[463] The Orwellian double speak involved here has drawn length criticism from *No CCTV* http://www.no-cctv.org.uk/blog/the_manufacture_of_surveillance_by_consent.htm

new legislation – meaning the public can be confident cameras are not there to spy on them but to protect them"[464]. However British citizens have not given their consent, it has merely been assumed. The inclusion of ANPR under the auspices of the code appears to have been an afterthought since there are only three mentions of ANPR in the twenty-five page report. None of the peculiar features of mass ANPR surveillance and its implications for privacy or human rights are addressed. The code of practice has no statutory basis and there is no punishment for breaching its recommendations.[465] The Protection of Freedoms Bill passed into law on May the 1st 2012. ANPR is still unregulated by statute.

The national ANPR network, is a core technology of 'ordinary' policing. It is primarily concerned with the everyday policing of: vehicle tax evasion; the detection of those driving vehicles without insurance and the tracking and tracing of those using their cars in commission of crime. These are all clearly legitimate aims of policing. As legitimate aims of 'ordinary' policing the mechanisms that service them deserve to be fully in the sphere of democratic accountability. However because ANPR sits at the intersection between ordinary crime and counter-terrorism and national security, transparency and accountability are obscured and undermined. Democracy would appear to be the loser.

The Protection of Freedoms Bill passed into law on May the 1st 2012. ANPR is still unregulated by statute.

Bibliography of Key Texts

Association of Chief Police Officers by the National Policing Improvement Agency (ACPO NPIA). (2009). “Practical Advice on the Management and Use of Automatic Number Plate Recognition.” Available at:

[464] https://www.gov.uk/government/news/surveillance-camera-code-of-conduct-comes-into-force
[465] http://amberhawk.typepad.com/amberhawk/2011/02/protection-of-freedoms-bill-promotes-efficient-cctv-surveillance-not-effective-privacy.html

http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf

ACPO (2010). “ANPR Strategy for the Police Service 2010-2013.” Available at: www.acpo.police.uk/documents/crime/2010/201010CRIANP01.pdf.

ACPO (2011). “National ACPO ANPR Standards (NAAS)”. Version 4.12. Available at:http://www.acpo.police.uk/documents/crime/2011/201111CBANAAS412.pdf

ACPO (2013) *The police use of Automatic Number Plate Recognition: A review by a working group of interested parties aimed at addressing concerns and providing understanding of the workings and regulation of the system*. Available at: http://www.acpo.police.uk/documents/crime/2013/201303CBA-ANPR.pdf

Birmingham City Council (BCC) (2010) Project Champion: Scrutiny Review into ANPR and CCTV Cameras, Birmingham City Council, 02 November 2010

British Society for Social Responsibility in Science (BSSRS) (1985) *TechnoCop: New Police Technologies*, BSSRS Technology of Political Control Group, London, Free Association Books.

Bunyan, T. (1977) *The History and Practice of The Political Police in Britain*, London, Quartet Books.

Butcher, L. (2009) 'Roads: Speed Cameras', *House of Commons Briefing Paper*, Standard Note: London, House of Commons Library.

Chief Constable of Devon and Cornwall v Information Commissioner and Mathieson [2012] UKUT 34 (AAC).

Graham, S. (2004). *Cities, War, and Terrorism: Towards an Urban Geopolitics*. London, Wiley.Grieve, D. & Laing, E. MP, (2010) *Reversing the Rise of the Surveillance State*, London, Conservative Party. Avialable at: http://conservativehome.blogs.com/files/surveillance-state.pdf

September 2009 Haines, A. and Wells, H. (2012) 'Persecution or protection? Understanding the differential public response to two road-based surveillance systems', *Criminology and Criminal Justice* 2012 12: 257.

Her Majesty's Inspectorate of Constabulary (HMIC) (2009) *Adapting to Protest – Nurturing the British Model of Policing,* London, HMIC. Available at: http://www.hmic.gov.uk/media/adapting-to-protest-nurturing-the-british-model-of-policing-20091125.pdf

House of Lords, (2009) *Surveillance: Citizens and the State* Volume I: HL Paper 18–I London : The Stationery Office. HL Paper 18–I

Independent Police Complaints Commission (IPCC) (2010) *Independent investigation into the use of ANPR in Durham, Cleveland and North Yorkshire from 23rd to 26th October*

Mathieson v Information Commissioner [2011] Appeal No. EA/2010/0174, heard before Alison McKenna, Tribunal Judge In the First-Tier Tribunal General Regulatory Chamber (Information Rights) 11 April 2011

Mathieson v Information Commissioner [2012] Appeal No. EA/2010/0174, heard before HH Judge Shanks In the First-Tier Tribunal General Regulatory Chamber (Information Rights) 18 June 2012

No-to-CCTV (2011) Royston's ANPR "Ring of Steel" - the shape of things to come? 13/6/2011. Available at: http://www.no-cctv.org.uk/blog/roystons_anpr_ring_of_steel_the_shape_of_things_to_come.htm

No CCTV (2013) *What's Wrong With ANPR?* Available at: http://www.no-cctv.org.uk/whats_wrong_with_anpr.asp

Officer of the Surveillance Commissioners (2012), *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012* Presented to Parliament pursuant to section 107(3) of the Police Act 1997, HC 498 SG/2012/127, London: The Stationery Office.

PA Consulting (2004) *Engaging criminality – Denying Criminals the Use of the Road, London,* PA Consulting Group. Available at:

http://www.popcenter.org/problems/residential_car_theft/PDFs/Henderson.pdf

PA Consulting (2004b) *Driving Down Crime Denying Criminals use of the roads,* London, PA Consulting Group, Available at:

http://www.popcenter.org/problems/residential_car_theft/PDFs/Henderson.pdf

Thornton, Sara. (2010). *Project Champion Review*, Thames Valley Police. http://www.statewatch.org/news/2010/oct/uk-project-champion-police-report.pdf

CREDIT SCORING

IRISS WP3 CASE STUDIES
"CASE STUDY SET 2: PRIVATE SECTOR → CITIZEN"

TASK 3.2

CASE STUDY: CREDIT SCORING IN AUSTRIA

INSTITUTE OF TECHNOLOGY ASSESSMENT

AUSTRIAN ACADEMY OF SCIENCES

Robert ROTHMANN

Jaro STERBIK-LAMINA

Walter PEISSL

VIENNA, 12/2013

Content

1 History and Implementation

- ***The history of the surveillance practice as used by a particular organization or public authority***
- ***When, where and how it has been implemented, who led the implementation***

The first organisation to initiate a database aiming at assessing the creditworthiness of customers in Austria was the so called 'Creditor Association for the Protection of Claims in Case of Insolvencies' (Creditorenverein zum Schutz der Forderungen bei Insolvenzen). Today, this organization is known as the 'Credit Protection Association' (Kreditschutzverband, KSV 1870).[466]

As the name indicates, the KSV was founded on April 10th, 1870 in Vienna. In their article, Krenn & Zeger (2009) claim that the KSV 1870 was the first such organization in Europe, whereas Knyrim (2008) also mentions the German organization 'United Credit Bureaus Bürgen' (Vereinigte Auskunfteien Bürgen) from 1862.

Similar Austrian institutions are the 'Creditreform' [467], founded in 1889, or the 'Carinthian Creditor Association' ("Kärntner Kreditorenverein"), established in 1924 and now known as 'Alpine Creditor Association for Credit Protection and Business Economics' (Alpenländischer Kreditorenverband für Kreditschutz und Betriebswirtschaft, AKV).[468]

Over time, the KSV 1870 gradually expanded its services. In 1913, the services 'encashment'/'collection' (Inkasso) and 'information/inquiry' (Auskunft) were added, and in 1955 a judicial representation for claims (gerichtliche Forderungsvertretung) was introduced. In 1964, the KSV finally began gathering information on private persons. The 'small loan cadastre' was established (known today as 'consumer credit registry'

466 http://www.ksv.at/KSV/1870/ (accessed 05 Oct. 2013).
467 http://www.creditreform.at/index.html (accessed 05 Oct. 2013).
468 http://www.akv.at (accessed 05 Oct. 2013).

(KonsumentenKreditEvidenz/ KKE), the list of unwanted accounting connections (Ungewollte Kontoverbindungen, UKV bzw. Warnliste der Banken, WL) was introduced, and since 1997, there is the 'goods credit registry' (WarenKreditEvidenz, WKE)[469], mainly used for mail order and telecom companies (cf. Krenn & Zeger 2009). The 'goods credit registry' also provides addresses and existence checks as a service for companies.

Another important actor was Deltavista. The Company was actually founded in 1994. In 2000, Deltavista opened an office in Vienna, Austria. In 2011, CRIF acquired Delta Vista Switzerland and Austria.[470] CRIF describes itself as a leading provider of credit management solutions in Europe. Its headquarters are located in Bologna, but there is also a branch office in Vienna.[471]

Besides a relatively small number of companies with their own data sets (about 5 - 7), a wide range of encashment services, detective agencies and other credit reference services offer economic information (cf. Krenn & Zeger 2009).

469 http://www.ksv.at/KSV/1870/de/1wirbieten/1auskuenfte/3datenbanken/wke.html (accessed 05 Oct. 2013).

470 https://www.deltavista.com/content/view/29/281/lang,ge/ (accessed 05 Oct. 2013).

471 **CRIF GmbH**, Diefenbachgasse 35, A-1150 Wien, DVR: 1062107, Tel. +43 (0)1 897 42440; www.crif.at

2 Stakeholders

- ***Who the key stakeholders in the surveillance practice are***

Group 1: Private Companies

The first group of stakeholders consists of different private companies providing services or selling goods (to consumers, small and medium-sized businesses and other companies). On one hand they like to have data on the credit rating of each customer to calculate their entrepreneurial risk, but on the other hand their business partners or banks and the financial market also rate them.

Pooled, this group of stakeholders includes:

- banks and other financial institutions (stocks, bonds and securities traders etc.)
- telecom-, leasing-, and insurance companies
- other businesses, corporations and companies providing payment by instalments or any other kind of business where payment occurs after delivery, and therefore generally want to know their business partners in order to minimize risk when dealing with them (online-sales, ...). [472]

In some cases, companies are forced to mitigate their risks by law (see below). In the end there are various companies which rate themselves against each other (rate and be rated), so the role of the rating operator and the concerned switches.

[472] In the case of insurance companies, the relation is somewhat different because the customer gives his money in the first place. Risk assessment by the insurance company nevertheless takes place in the background.

Group 2: Consumers and Consumer Protection Organizations

- Consumers: want to know what data are collected about them, exercise their rights in regard to rectification and deletion of data, or wish to buy services and goods at the same price and conditions as others.
- Consumer- and credit user protection departments as well as Non-Government or Non-Profit Organizations (NGO's & NPO's): protecting consumer and credit user rights; suing big companies in test or precedence cases; helping consumers and credit users by providing guidance on how to exercise their rights:
    - Chamber of Labor (Arbeiterkammer, AK)[473]
    - Association for Consumer Information (Verein für Konsumenteninformation, VKI)[474]
    - The Austrian Federal Economic Chamber (Wirtschaftskammer Österreich, WKO) [475]
    - ARGE DATEN - Austrian Society for Data Protection (Österreichische Gesellschaft für Datenschutz) [476]
    - Quintessenz - Association for the Restoration of Civil Rights in the Information Age (Verein zu Wiederherstellung der Bürgerrechte im Informationszeitalter)477; Quintessenz also runs the Austrian 'Big Brother Awards' [478]

Group 3: Regulatory Organisations and Institutions

The main regulatory organisations are

[473] http://www.arbeiterkammer.at/index.html (accessed 05 Oct. 2013).
[474] http://www.konsument.at/cs/Satellite?pagename=Konsument/Page/Start (accessed 05 Oct. 2013);
see also http://verbraucherrecht.at/cms/index.php?id=121 (accessed 05 Oct. 2013).
[475] http://portal.wko.at/wk/startseite.wk (accessed 05 Oct. 2013).
[476] http://www.argedaten.at/php/cms_monitor.php?q=AD-NEWS-LAST (accessed 05 Oct. 2013).
[477] http://www.quintessenz.at/cgi-bin/index (accessed 05 Oct. 2013).
[478] http://www.bigbrotherawards.at/2013/ (accessed 05 Oct. 2013).

- the Austrian Central Bank (National Bank of Austria, Österreichische Nationalbank, OeNB) [479]
- the Austrian Financial Market Authority (Finanzmarktaufsicht, FMA) [480]
- the Austrian Data Protection Commission (Datenschutzkommission, DSK) [481]

Group 4: Private Credit and Debt Collection Agencies

There are several credit agencies, information brokers and debt collecting agencies (Inkassobüros) whose business is to provide credit ratings, risk management services, solvency and address information on (potential) customers, as well as helping creditors to get back their money (enchashment).

- Aktiva Inkassobüro GesmbH & Co KG[482]
- Alpenländischer Kreditorenverband für Kreditschutz und Betriebswirtschaft (AKV)[483]
- Auskunftei GmbH Eder Christian, Bruck-Großglockner[484]
- Auskunftei Lux staatl konz cand jur K.G. WRBA[485]
- AVS Betriebsorganisation Ges.m.b.H. [486]
- Bisnode Austria Holding GmbH, Vienna (Dun & Bradstreet Austria)[487]
- Creditreform Wirtschaftsauskunftei Kubicki KG[488]
- CRIF489 (formerly Delta Vista[490])
- Coface Austria Kreditversicherung Service GmbH, Vienna[491]
- infoscore austria gmbh[492]

[479] http://www.oenb.at/ (accessed 05 Oct. 2013).
[480] http://www.fma.gv.at/de/startseite.html (accessed 05 Oct. 2013);
[481] https://www.dsk.gv.at/DesktopDefault.aspx?alias=dsk (accessed 05 Oct. 2013).
[482] http://www.aktiva-inkasso.at (accessed 05 Oct. 2013).
[483] http://www.akv.at/ (accessed 05 Oct. 2013).
[484] http://www.spuernase.at/index.html (accessed 05 Oct. 2013).
[485] http://www.detektei-lux.at/ (accessed 05 Oct. 2013).
[486] http://www.avs-europe.com/index.php?at_start (accessed 05 Oct. 2013).
[487] http://www.bisnode.at/ (accessed 05 Oct. 2013).
[488] http://www.creditreform.at/index.html (accessed 05 Oct. 2013).
[489] http://www.crif.at/Pages/default.aspx (accessed 05 Oct. 2013).
[490] https://www.deltavista.com/content/view/15/34/lang,ge/ (accessed 05 Oct. 2013).
[491] http://www.coface.at/ (accessed 05 Oct. 2013).
[492] http://www.arvato-infoscore.at/ (accessed 20 Nov. 2013).

- Intrum Justitia GmbH[493]
- IS Inkasso Service GmbH, Inkassoservice & Auskunftei für Kreditverhältnisse, Linz [494]
- Kreditschutzverband von 1870 (KSV 1870)[495]
- P & P Wirtschaftsdetektive und Auskunftei GmbH, St. Pölten [496]
- payolution GmbH, Vienna [497]
- PROINFORM Wirtschaftsinformationen GmbH, Neumarkt/Wallersee [498]
- Progress West Inkassoinstitut u Auskunftei GmbH, Salzburg [499]
- Schimmelpfeng Auskunftei GmbH, Vienna
- Top Inkasso & Auskunftei Ges z Schutz d Gläubiger, Salzburg
- ...

Furthermore, there is a small group of companies providing software solutions and tools to conduct the actual analyses:

- DATA TECHNOLOGY Betriebsberatungs GmbH & Co KG[500]
- EMEA SmartStream Technologies Austria[501]
- Informa Unternehmensberatung GmbH (currently in liquidation)
- ...

[493] http://www.intrum.com/at/(accessed 20 Nov. 2013).
[494] http://www.inkasso.at/index_at.php (accessed 05 Oct. 2013).
[495] http://www.ksv.at/KSV/1870/ (accessed 05 Oct. 2013).
[496] http://www.arge-wirtschaftsdetektive.at/ (accessed 05 Oct. 2013).
[497] http://www.payolution.com/ (accessed 05 Oct. 2013).
[498] http://www.auskunftei.at/ (accessed 05 Oct. 2013).
[499] http://www.progresswest.at/ (accessed 05 Oct. 2013).
[500] http://www.datatechnology.at/main.asp?VID=1&kat1=94&kat2=666&kat3= (accessed 05 Oct. 2013).
[501] http://www.smartstream-stp.com/ (accessed 05 Oct. 2013).

3 Regulation

- ***How has it been shaped for a particular use***
- ***How it is currently regulated***

As a result of mergers, name changes, relocation of offices, cooperation and joint ventures as well as the sale of databases, the market is cluttered and the responsible stakeholders changed repeatedly. In addition, enhanced internationalization is emerging. By transferring their data stocks to companies based in foreign countries like Germany or Slovakia, the Austrian data protection regulations can be circumvented (cf. Krenn & Zeger 2009).

As the Austrian history of credit bureaus and the establishment of the Basel Committee on Banking Supervision shows, there is a gradual refinement of rating and scoring methods and an approximation of credit assessment applications for the retail market and private persons. Furthermore, it can be said that there is increasing transparency and regulation, even though these developments have not necessarily created a balanced power relation between credit scoring agencies and the concerned individuals.

The most important regulation comes from the 'Basel Committee on Banking Supervision' (BCBS).[502] The so-called 'Basel Accord' is a credit risk framework introduced in 1988 by which the Basel Committee on Banking Supervision defined capital standards for international banks in member countries (G-10 countries). Austria is not part of the committee.

The objective was to limit the banks' business risks by banking supervision and strengthen the financial system overall. In order to meet the requirements of ongoing developments in

[502] http://www.bis.org/bcbs/ (accessed 05 Oct. 2013).

banking, the Basel Committee began revising these requirements in 1999, and the new capital accord ('Basel II') came into effect in 2007. [503]

The requirements of the new accord serve to increase the stability of the international financial system by introducing more risk-sensitive minimum capital charges for exposures, expressly accounting for operational risks, reinforcing the role of financial market supervision and increasing market transparency. In a parallel process, the European Union (EU) developed the Capital Requirements Directive (CRD), which pursues the same objectives and applies to all banks and investment firms in the EU once it has been implemented in the national legislation of Member States.[504] In December 2010, the preliminary version of Basel III was published. Basel III shall come into force in 2014.

The Austrian National Bank (OeNB) and the Financial Market Authority (FMA) require banks to maintain certain standards in the granting of loans. The auditor must obtain an overview of the structure of the bank's internal control system and the adequacy of the relevant control measures for rating systems. Audit priorities include the development of the rating methodology, on-going validation and the rating allocation. These standards and regulations, however, are less focused on data protection and ethical criteria than on the solvency of the bank and the stability of the financial market, e.g. assessment of cluster risk – susceptibility of far reaching default payments of certain customer groups. To avoid such risks, a heterogeneous customer base is recommended. All this makes it ultimately necessary to know as much as possible about the customer (see also 'know your customer' - policy; money laundering/terrorism financing). The economic stability of the financial market is therefore in contradiction with individual rights and the confidentiality of personal data.

[503] Basel Committee on Banking Supervision (2004): *International Convergence of Capital Measurement and Capital Standards – a Revised Framework*, Bank for International Settlements, Press & Communications, CH-4002 Basel, Switzerland, ISBN: 92-9197-669-5.
[504] http://www.oenb.at/de/finanzm_stab/basel_2/basel_ii.jsp (accessed 05 Oct. 2013).

Furthermore the DSK issued several decisions on data handling and data processing in conjunction with the granting of credits, like [505]

- Decision K600.033-018/0002-DVR/2007 on the right to access, data on financial solvency, scoring, automated individual decision;
- Decision K600.014-010/0002-DVR/2007 on negative lists, blacklisting, solvency;
- Decision K211.773/0009-DSK/2007 on data flow, worthiness of protection;
- Decision K121.348/0007-DSK/2008 on right to access, lacking completeness of contents, telecom companies, credit agency as a service provider, data on financial solvency, scoring-value, principal role in credit checks, automated individual decision.

External Accountability

- Whether the practice is externally accountable and if so, to whom

The practice of credit scoring and rating by banks and credit agencies is accountable to regulative organisations like the Data Protection Commission (DSK), the Financial Market Authority (FMA) or the Austrian National Bank.

Credit agencies repeatedly and unlawfully refuse the deletion of data from their "black" lists. Several Supreme Court decisions have clearly established that a complete deletion of entitlement exists (cf. OGH 6 Ob 195/08g, 1.10.2008; OGH 6Ob41/10p, 15.4.2010).[506]

There is the possibility of compensation for illegal or wrong entries in 'warning lists' and databases. If an interested party is harmed by an entry in such a database, because it can not claim, for example, a cheap mobile phone offer and therefore needs to choose a much

[505] http://www.ris.bka.gv.at/ (accessed 20 Nov. 2013).
[506] http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=30575bvj (accessed 28 Nov. 2013).

more expensive option, he can hold somebody accountable for these damages (Credit damage according to § 1330 ABGB).[507]

Legal Framework

Several laws, directives and regulations have to be taken into account:

- Basel I + II + III (Basel Committee on Banking Supervision – BCBS) [508]

European Directives [509]

- Directive 2008/48/EC on credit agreements for consumers
- Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions (cf. Article 8)
- Directive 2006/49/EC on the capital adequacy of investment firms and credit institutions
- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (cf. Article 15 - Automated Individual Decisions)

Directive 95/46/EC - Article 15 - Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

[507] http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=30575bvj (accessed 20 Nov. 2013).
[508] The full name is "International Convergence of Capital Measurement and Capital Standards – a Revised Framework"; June 2004, the Basel Committee on Banking Supervision, BIS.
[509] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed 05 Oct. 2013).

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

National Laws [510]

- Banking Act (Bankwesengesetz, BWG) cf.§ 39;
- Trade Regulation (Gewerbeordnung 1994, GewO), cf. § 152;
- Consumer Credit Act (Verbraucherkreditgesetz, VKrG)
- Data Protection Act (Datenschutzgesetz 2000, DSG), cf. § 49;
- Gambling Act (Glücksspielgesetz, GSpG)
- Loan and Credit Law Amendment Act (Darlehens- und Kreditrechts-Änderungsgesetz, DaKRÄG)
- Solvency Regulation (Solvabilitätsverordnung, SolvaV)

Use of credit rating is not only possible - see for example § 152 Trade Regulation (GewO) 1994 – , but even explicitly required in some cases, for instance with regard to gambling (see § 25 Gambling Act). The failure to obtain required background information on creditworthiness of customers may result in legal consequences (cf. Bydlinski 2008; Knyrim 2008).

[510] http://www.ris.bka.gv.at/ (accessed 20 Nov. 2013).

4 Credit Assessment

Blacklists

As a key player the KSV1870 provides a range of different services including domestic and international credit reports, address and existence checks, credit assessment for companies and private persons, solvency monitoring over time, domestic and international debt collection as well as person-related data for marketing purposes.[511]

In the context of private persons the KSV1870 operates three relevant services:

- the 'consumer credit registry' (KonsumentenKreditEvidenz, KKE)
- the 'list of unwanted accounting connections' (Warnliste der Banken, WL)
- the 'goods credit registry' (WarenKreditEvidenz, WKE)

The 'consumer credit registry' (KonsumentenKreditEvidenz, KKE) exists since 1964 and includes information on every consumer credit in Austria. Banks transmit full credit data and personal data as well as potential arrears with payments. It is estimated, that the register, has more than two million entries. [512]

With the 'list of unwanted accounting connections' (Warnliste der Banken, WL) banks alert each other on customers which are in arrears with payments and provide hints on repudiatory breaching of contracts.

The 'goods credit registry' (WarenKreditEvidenz, WKE) is a data application which includes business cases where customers got goods or services on open account (about 300,000 entries).[513]

[511] https://www.ksv.at/ (accessed 05 Oct. 2013).
[512] http://diepresse.com/home/meingeld/verbraucher/642381/Schwarze-Listen_Sie-sind-leider-nicht-kreditwuerdig (accessed 20 Nov. 2013).
[513] DiePresse.com (06.08.2008): Datenschutz: „Schuldenfrei“, einfach so, http://diepresse.com/home/wirtschaft/economist/404298/Datenschutz_Schuldenfrei-einfach-so?from=suche.intern.portal (accessed 10 Nov. 2013).

Rating and Scoring

The above mentioned services are not defined as rating or credit scoring but function as blacklists or warning lists. The KSV1870 also offers rating of companies. For the calculation of the score more than 20 factors get specifically weighted and combined. [514] However, the actual operation of the rating is not disclosed on the website. According to research conversations the information on the actual rating process is kept from the public to avoid any manipulation of the rating. The rating process is also viewed as a business secret (like e.g. the Google search algorithm).

Rating is defined as assessment of the current or future ability of a company or private person to pay (Bornett et al. 2006). When one wants to predict credit risk, one is interested in predicting the potential loss that might occur. Therefore the most popular credit risk parameter is the default probability. The credit quality of a borrower also depends on the exposure-at-default, the outstanding and unsecured credit amount at the event of default, and the loss-given-default, which usually is defined as a percentage of the exposure-at-default (cf. Hayden 2003).

The Basel Guidelines differ between several types of risks like claims on sovereigns, claims on non-central government public sector entities, claims on multilateral development banks, claims on banks, claims on securities firms, claims on corporates, claims included in the regulatory retail portfolios, claims secured by residential property or claims secured by commercial real estate (cf. Basel Committee on Banking Supervision 2004).
In the corporate sector each branch applies different benchmarks. The borrower is measured at the benchmark of the relevant branch (cf. Bornett et al. 2006).
There is also a differentiation between bank-internal ratings (IRB-Approach) and bank external ratings (by agencies) (cf. Basel Committee on Banking Supervision 2004).

[514] https://www.ksv.at/ksv1870-rating (accessed 05 Oct. 2013).

The exact scoring method as well as used input variables, depend on whether a private person or a company is rated, as well as on the individual loan type and parameters (foreign currency loans, euro loans, amount and purpose of loan, ...).
In the retail segment, it is distinguished between mass-market banking and private banking. Mass-market banking refers to general (high-volume) business transactions with retail customers. For the purpose of credit assessment, we can differentiate the following standardized products in this context: current accounts, consumer loans, credit cards and residential construction loans. Private banking involves transactions with high-net-worth retail customers and goes beyond the standardized products used in mass-market banking (cf. Thonabauer et al. 2004).

A general methodical step in credit scoring is the differentiation between hard facts (quantitative analysis of creditworthiness) and soft facts (i.e. qualitative information).
The rating models of banks consider, in simplified terms, the following factors: hard facts, soft facts, warning notices (cf. KKE, WL, WKE) and securities (cf. Bornett et al. 2006).
According to Hayden (2003) there are three main possible model input categories: accounting variables, market based variables such as market equity value and so-called soft facts such as the firm's competitive position or management skills.

Hard facts

The quantitative factors are primarily derived from the analysis of annual accounts (balance sheet analysis). The hard facts get transformed into operating numbers or key performance indicators and are assigned to analytical classes. Important indicators are, for example: percentages of effort; return on sales; cash-flow; debt service limit; equity; mobility; asset coverage; debtor days; creditor days, the size of the company and duration of storage (cf. Strobl & Hahn 2010; cf. Bornett et al. 2006).
As standardized documents (such as annual financial statements in the corporate customer segment) are not available for the evaluation of a retail customer's financial situation, it is

necessary to assess these customers on the basis of information they provide regarding their assets and liabilities (cf. Thonabauer et al. 2004). During the term of the credit transaction, the lender should evaluate activity patterns in the customer's current account on the quantitative level. This will require historical records of the corresponding account data. Examples of the information to be derived from these data include overdraft days as well as debit and credit balances, which make it possible to detect payment disruptions at an early stage (cf. Thonabauer et al. 2004). In the context of credit cards the institutions should assess the customers transactions and purchasing behaviour (cf. Thonabauer et al. 2004).

Soft facts

Soft facts can be classified into three levels: the personality of the businessman and the management skills; operational and technical indicators; the economic environment (cf. Strobl & Hahn 2010).

Personal soft fact indicators (among medium-sized businesses) are e.g. decisiveness and creativity, innovation capability and flexibility, leadership and assertiveness, foresight and resilience, risk tolerance and succession planning (cf. Strobl & Hahn 2010).

To recognize problem loans it is recommended, for example, to consider the following personal symptoms: reticence/dwindling willingness to talk, personal and family problems, health, age, lifestyle – hobbies, public engagement, passion for gambling, divorce, convictions (cf. Strobl & Hahn 2010). In this context we have to mention that the European data protection directive defines health information as sensitive data (cf. Directive 95/46/EC Article 2, Definitions).

An essential qualitative element in retail credit assessment is socio-demographic information (age, profession, marital status, gender, duration of employment, length of residence; etc.). If the customer relationship has existed for some time, it is advisable to assess the type and history of the relationship (cf. Thonabauer et al. 2004).

All these variables get statistically transferred and weighted according to the type of credit. Especially the weighting of information makes the rating process a hidden procedure.

Models

Commonly used credit assessment models are: heuristic models (classic rating questionnaires, qualitative systems, expert systems, fuzzy logic systems), statistical models (multivariate discriminant analysis, regression models, artificial neural networks), causal models (option pricing models, cash flow models) and hybrid forms (cf. Thonabauer et al. 2004).

Heuristic models are also known under the heading of 'expert systems'. The quality of heuristic models depends on how accurately they depict the subjective experience of credit experts. Therefore, not only the factors relevant to creditworthiness are determined heuristically, but their influence and weight in overall assessments are also based on subjective experience.

While heuristic credit assessment models rely on the subjective experience of credit experts, statistical models attempt to verify hypotheses using statistical procedures on an empirical database. The accuracy of fit of any statistical model thus depends heavily on the quality of the empirical data set used in its development (level of measurement, assumption of normal distribution of specific variables or indices, large enough data sets to enable statistically significant statements...). For example, default data on governments and the public sector, financial service providers, exchange-listed/international companies, as well as specialized lending operations are rarely available in a quantity sufficient to develop statistically valid models. In addition to the required data quantity, the representativity of data has to be taken into account (cf. Thonabauer et al. 2004).

The biggest drawback of hard facts is the focus on data from the past (cf. Strobl & Hahn 2010). Other critical aspects are the completeness of data, the factual data accuracy and the probability of mistaken identities. The Austrian data protection act rules this by paragraph 6

(cf. Sachliche Datenrichtigkeit, § 6 Abs. 1 Z 4 DSG). However the actual practical recognition is questionable.

Historically banks used to rely on the expertise of credit advisors who looked at a combination of accounting and qualitative variables to come up with an assessment, but especially larger banks switched to quantitative models during the last decades (cf. Hayden 2003).

In terms of discriminatory power and calibration, statistical models demonstrate superior performance compared to heuristic models. Therefore, banks are increasingly replacing or supplementing heuristic models with statistical models in practice. This is especially true in those segments for which it is possible to compile a sufficient data set for statistical model development (in particular corporate customers and mass-market banking). For these customer segments, statistical models are standard (cf. Thonabauer et al. 2004).

According to research conversations automated decisions seem to be the standard process of credit assessment in the retail segment, whereas human decisions seem to be the exception. Just in cases where the actual credit score obviously is in contradiction to real life conditions of a customer, closer attention will be paid. Instead, non-automated human decisions are treated as highly biased because they depend on the subjective know how and experience of the credit manager.

Rating levels are usually based on a school grading system, intermediate grades can be inserted (cf. Strobl & Hahn 2010):

0.0 unrated

0.5 risk free (external AAA or guarantee of authority)

1.0 excellent solvency

1.5 very good solvency

2.0 good solvency

2.5 average solvency

3.0 moderate solvency

3.5 poor solvency

4.0 very poor creditworthiness

4.5 critically endangered

5.0 insolvency or similar proceedings / failure according to Basel II

Increased attention should be turned to borrowers with a rating of 3,5 and more (cf. Strobl & Hahn 2010).

For the concerned customer the result of the rating process has an influence on the adduced securities and the interest rate (cf. Bornett et al. 2006). Further implications of a bad credit score are a general exclusion from economic participation and in particular, the refusal of account opening, refusal of further loans and credits, refusal of phone contracts, refusal of purchasing by mail order, a deterioration of payment terms, a deterioration of procurement terms and withdrawal of loyalty cards

5 Transparency: Watchers and Watched

Several bigger credit agencies and organisations like the KSV1870 or CRIF offer some information on their websites, including details on subject access requests or name and function of different services, databases and warning lists.

More specific information can be found in the Basel Guidelines and on the websites of regulators (cf. Thonabauer et al. 2004, cf. Thonabauer et al. 2006). Documents from the National Bank (OeNB) and the Financial Market Authority (FMA) also include sections and chapters on assessing the rating models' suitability and the problem of fulfilment of essential methodological requirements (cf. Thonabauer et al. 2004).

During the study we visited and called some banks and asked for experts or someone who knows more about the process of credit scoring in general. The bank staff named neither competent persons nor departments. The staffs seem to be trained to refuse such inquiries. It is said, that they do not know who is responsible and they do not know whom to ask. The information is kept from the public to avoid any manipulation of the rating. The actual rating-process is seen as a business secret like the Google algorithm.
Finally, credit assessment is much about trust/mistrust (latin: creditum = in good faith entrusted, latin: credo = believe).[515] The customer is distrusted.

Since credit scoring is a complex, abstract and hidden surveillance practice, there is a clear information gap between the watchers and the watched. It is even hard to provide scientific evidence for the existence of certain data sets and databases. Furthermore it is difficult to get some information on the actual use of these data in terms of scoring methods (weighting factors) as well as on the actual border between human decisions and automated decisions (cf. Directive 95/46/EC, Article 15) in everyday routines of credit assessment. Information on these issues is not accessible without good relations to a gatekeeper or insider. While the customer is entirely transparent, the rating system itself is not.
Therefore Butschek (2008) also claims disclosure- and information symmetry.

Nevertheless the topic is open for discussion although there seems to be no deeper debate about discriminatory aspects. In this context reference is made to ARGE DATEN (Austrian Society for Data Protection), which leads the critical legal discourse on credit scoring in Austria. [516]

The actual process and method used to compute the individual credit score is a business secret. Customers don't know what information is actually stored about them and if they do

[515] http://www.duden.de/rechtschreibung/Kredit_Finanzierung_Anleihe (accessed 20 Nov. 2013).
[516] http://www.argedaten.at/php/cms_monitor.php?q=AD-NEWS-LAST (accessed 05 Oct. 2013).

so, they don't know how the information is used and weighted. A negative credit score may be perceived as unfair, especially by the concerned, but the process of scoring itself is not much criticized as a surveillance practice (cf. Resilience). However there is no empirical evidence in terms of representative survey data on the public opinion.

Subject Access Requests

- How subject access requests feature, and what are the rates of use

According to the Austrian Data Protection Act, consumers have the right to request a copy of all data held on them by the credit bureau. This is for free once a year and has to be done within 8 weeks.

Most rating organisations like the KSV1870 or CRIF offer the possibility for subject access requests (self-disclosure) for private persons and companies on their websites. Furthermore they sometimes list some information on their rating models as well as a few legal basics.

In the course of the study tow subject access requests were conducted by one of the authors; one at the KSV1870 and the other one at CRIF. Both were for free and in time as the data protection act directs. The KSV1870 listed my current post address and a few service companies, which are involved in the processing of my data. The CRIF revealed all my main addresses since I was born. In both cases they revealed no further information on how they use these data or how, for example, my current postcode is used and weighted in the rating process. They also claim to have not saved any payment experience data on my person.

It was also asked for the rates of use of subject access requests (self-disclosure), and if there was an increase over the last years, but such information will not be published by the KSV. CRIF Austria let us know by its CEO that about 10.000 subject access requests have to be answered each year.

7 Credit Scoring and Resilience

- What controversies have arisen in the history of that surveillance practice

- Which type of resilience is relevant to credit scoring

The Term 'Resilience' comes from the Latin word 'resilire' that means 'to return', 'to put back' or 'to jump back'.[517] The German dictionary Duden defines 'Resilienz' as psychic ability to recover, and a kind of resistibility or power to resist. One could also say it is the ability to withstand and survive difficult life situations or conditions without any further continual interference or impairment.

If we understand resilience as ability to recover from stress, or as a process of coming back into a stable condition or constitution, we have to ask what stress or unstable constitution means and should consider that surveillance could be seen as such a stress producing element. Taking this into account, resilience in surveillance societies appears in four different ways:

1: Surveillance as an intervention, which reduces stress;
(a kind of helpful tool to civilise society; civil refinement);
If we understand surveillance as an intervention or (preventive) method to reduce stress, resilience can be seen as the positive outcome of these efforts in reducing crime or other social threats; increased resilience means increased safety, security and economic efficiency;
If we understand surveillance as an intervention which reduces stress and leads to increased social and economic stabilisation, resilience can also be seen as a process of

[517] http://www.duden.de/suchen/dudenonline/resilienz (accessed 10. Oct 2013).

habituation and customisation, a process of getting used to surveillance after implementation; therefore surveillance is experienced as something new but nothing bad;

2: Surveillance as an intervention, which produces stress;

(surveillance as privacy invasive intervention and measure of authoritarian control).

If we understand surveillance as an intervention which produces stress, than resilience could mean a kind of chilling effect or suppression; a process of falling into a situation or social constitution with losing ability to react or express critique; a kind of homogenisation and/or stagnation of social, economic and democratic processes; (this also includes forms of discrimination and exclusion);

If we understand surveillance as an intervention, which produces stress, resilience can also be seen as a kind of increased awareness against such privacy invasive and discriminative methods; resilience then means a critical discourse against such surveillance practices and a kind of resistance; this also includes the discourse on consumer protection, data protection and constitutional law;

As an international controversy the financial market crisis from around 2008 brought up the issue of easy lending, toxic assets and payment default. In that discourse society takes harm by less surveillance. That means private persons and companies should be monitored and rated as much and as deep as possible. The practice of rating and credit scoring is seen as a helpful and necessary method to avoid payment default and destabilization of the financial market.

The financial crisis also led to an increased public discussion on the power of rating, the used methods, possible bias-problems, and the influence on the economic situation (of national states) in a sense of a self-fulfilling prophecy. Nevertheless there is no questioning of rating and scoring in general. The debate just requests a more objective rating and more transparency.

As an Austrian specific controversy we would like to refer to a court case of illegal data reselling which took place in October 2013 in Vienna. In total 14 persons including bailiffs, court clerks and office workers of several district courts, have copied and sold information about non-public execution proceedings from juridical databases. From 2002 to 2010 execution data from nearly 40,000 legal and 92,000 private persons have been collected and resold with a total profit of about 300,000 Euros. The data were forwarded to banks and telecom providers. The judicial officers were finally found guilty in abuse of authority and breaching of official secrecy. They were sentenced to conditional imprisonment of between six to 24 months.[518] Some of the court clerks showed a barely pronounced sense of wrongdoing in front of the judge.[519]

There seems to be a strong understanding of the necessity of rating and scoring processes to ensure a secure financial system. It is obvious that lending money is a sensitive issue and that customers can't be trusted without any further securities. Concerned persons are outraged when they get no credit, but even the group of the watched seems to accept the system-inherent need for assessing the creditworthiness before lending money.

[518] DiePresse.com (15.10.2013): Schuldsprüche im Prozess um Justizdaten-Affäre, http://diepresse.com/home/panorama/oesterreich/1464663/Schuldspruche-im-Prozess-um-JustizdatenAffaere?from=simarchiv (accessed 10 Nov. 2013).
[519] DiePresse.com (09.10.2013): Gerichtsvollzieher verkauften Justizdaten: "Na und ...?", http://diepresse.com/home/panorama/oesterreich/1462796/Interne-Justizdaten-verkauft_Na-und- (accessed 10 Nov. 2013).

8 Media Coverage

- ***How, where and when it has been referred to in the media***
- ***How the organization or public authority has engaged with the public around its use of the surveillance practice***
- ***How members of the public have engaged with their data doubles and the organisations that use the surveillance practice***

Most of the newspaper articles relate to the financial crisis and the rating of sovereigns and banks. Those articles are not considered in the following list. Only a small part of the media coverage refers to the retail sector and personal loans. In these cases, credit scoring is not discussed as surveillance practice. The discourse mainly is about the difficulty to get credit for private persons and SMEs. Occasionally there are reports on data protection problems. A case of unauthorized data reselling in judicial circles was recently taken to court.[520]

Sample

Wirtschafts-Blatt (10/2013): Final in the trial on the Justice Data affair [521]

Justice. The verdict in the trial on the Justice Data affair, is imminent. The prosecutor sees "quite clear abuse," the defence lawyer asks for lenient sentences.

Die Presse (10/2013): Affair of data trading: "Justice loses confidence" [522]

[520] http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=95512otn (accessed 10 Oct. 2013).
[521] Wirtschafts-Blatt (15.10.2013): Finale im Prozess um Justizdaten-Affäre; http://wirtschaftsblatt.at/home/nachrichten/oesterreich/1464705/Finale-im-Prozess-um-JustizdatenAffaere?from=suche.intern.portal (accessed 10 Nov. 2013).
[522] Die Presse.com (08.10.2013): Affäre um Datenhandel: „Justiz verliert Vertrauen", http://diepresse.com/home/panorama/oesterreich/1462253/Affaere-um-Datenhandel_Justiz-verliert-Vertrauen?from=suche.intern.portal (accessed 2 Dec. 2013).

In Vienna, the penal procedure against 13 judicial clerks, who sold personal data of execution proceedings to a data company, began. The defendants say they have thought it was allowed.

Die Presse (10/2013): Data theft: Main accused committed suicide-attempt[523]

Main defendent at start of the process in hospital. 13 judicial officers are said to have illegally sold 133,000 records to credit reporting agency.

Die Presse (10/2013): Bailiff sold justice data, "So what ...?"[524]

In the court case on the systematic sale of data from execution-processes, some of the accused judicial officers showed a barely pronounced sense of wrongdoing.

Die Presse (08/2013); The data collectors: Who else collects and how to inquire there[525]

In addition to the Austrian authorities a range of private companies save data of citizens. They must also provide information. Even in the case of U.S. intelligence agencies, there is the - theoretical - possibility to request.

Wirtschafts-Blatt (07/2013): Corporate loans further difficult to obtain[526]

Study. According to the OeNB, Austrian banks have slightly tightened their credit standards in corporate business for the fifth time in a row.

---

[523] DiePresse.com (08.10.2013): Datendiebstahl: Hauptangeklagter beging Suizid-Versuch, http://diepresse.com/home/panorama/oesterreich/1462118/Datendiebstahl_Hauptangeklagter-beging-SuizidVersuch?from=suche.intern.portal (accessed 10 Nov. 2013).
[524] DiePresse.com (09.10.2013): Gerichtsvollzieher verkauften Justizdaten: "Na und ...?", http://diepresse.com/home/panorama/oesterreich/1462796/Interne-Justizdaten-verkauft_Na-und- (accessed 10 Nov. 2013).
[525] DiePresse.com (17.08.2013): Die Datensammler: Wer sonst noch speichert und wie man dort nachfragt. http://diepresse.com/home/panorama/oesterreich/1442439/Die-Datensammler_Wer-sonst-noch-speichert-und-wie-man-dort-nachfragt?from=simarchiv (accessed 20 Nov. 2013).

[526] Wirtschafts-Blatt (24.07.2013): Firmenkredite weiter schwer zu bekommen,

http://wirtschaftsblatt.at/home/nachrichten/oesterreich/1433967/Firmenkredite-weiter-schwer-zu-bekommen?from=suche.intern.portal (accessed 20 Nov. 2013).

derStandard (07/2013): Data breach - BAWAG strikes off AMS employees overdrafts[527]

AMS employees automatically lose their overdraft facility - data protection activist Zeger: "impudence and legally questionable"

Die Presse (04/2013): Lending: Companies are "unfaithful"[528]

According to a KSV survey, the loyalty to the bank decreases greatly.

Wirtschafts-Blatt (04/2013): Business loans are cheap - but rare[529]

The banks are more restrictive in the allocation of corporate loans. And nothing will change so quickly. Further tightening is expected.

Wirtschafts-Blatt (04/2013): Banks remain careful in lending[530]

Banks. Austria's banks are further tightening their corporate lending guidelines.

Die Presse (04/2013): Austria's banks are tightening credit standards[531]

The already restrictive lending practices of institutions is again tightened. The demand of firms diminishes because of economic risks.

Die Presse (01/2013): More company bankruptcies, but less private insolvencies[532]

---

[527] derStandard.at (26. Juli 2013): Datenpanne - BAWAG streicht AMS-Mitarbeitern Überziehungsrahmen, http://derstandard.at/1373513785006/Datenpanne---BAWAG-streicht-AMS-Mitarbeitern-Ueberziehungsrahmen (accessed 10 Nov. 2013).

[528] Die Presse.com (02.04.2013): Kreditvergabe: Firmen werden „untreu“, http://diepresse.com/home/wirtschaft/economist/1383568/Kreditvergabe_Firmen-werden-untreu?from=simarchiv (accessed 20 Nov. 2013).

[529] Wirtschafts-Blatt (25.04.2013): Firmenkredite sind billig - aber rar, http://wirtschaftsblatt.at/archiv/printimport/1393930/Firmenkredite-sind-billig-aber-rar?from=suche.intern.portal (accessed 20 Nov. 2013).

[530] Wirtschafts-Blatt (24.04.2013): Banken bleiben bei Kreditvergabe vorsichtig, http://wirtschaftsblatt.at/home/nachrichten/oesterreich/1393461/Banken-bleiben-bei-Kreditvergabe-vorsichtig?from=suche.intern.portal (accessed 20 Nov. 2013).

[531] Die Presse (24.04.2013): Österreichs Banken verschärfen Kreditrichtlinien http://diepresse.com/home/meingeld/finanzierung/1393478/Osterreichs-Banken-verschaerfen-Kreditrichtlinien?from=suche.intern.portal (accessed 20 Nov. 2013).

Last year, 6266 companies have been insolvent, 10,545 private could not pay their bills. Viennese are twice as likely bankrupt as the Austrian average, says Credit Reform.

Wirtschafts-Blatt (10/2012): Tough business with corporate loans continues[533]

Financing. In Austria banks report of restraint in corporate loans, according to ECB mainly SMEs are concerned.

Die Presse (07/2012): Hard times for debtors[534]

According to National Bank, banks have tightened the guidelines for corporate and household loans. This is evident from the quarterly survey of the OeNB on credit managers of leading banks.

Die Presse (03/2011): Blacklists: "You are unfortunately not creditworthy"[535]

Who landed on a blacklist, often does not get billed upon delivery or does not receive a cell phone contract. What to do in such a case?

Die Presse (07/2009): On banks the next hurricane occurs[536]

Austria's government is well advised to work within the EU for a relaxation of credit rules.

---

[532] DiePresse.com (15.01.2013): Mehr Firmenpleiten, aber weniger Privatinsolvenzen, http://diepresse.com/home/wirtschaft/economist/1332831/Mehr-Firmenpleiten-aber-weniger-Privatinsolvenzen?from=simarchiv (accessed 20 Nov. 2013).

[533] Wirtschafts-Blatt (31.10.2012): Weiter zähes Geschäft mit Unternehmenskrediten,

http://wirtschaftsblatt.at/home/nachrichten/oesterreich/1307367/Weiter-zaehes-Geschaeft-mit-Unternehmenskrediten?from=suche.intern.portal (accessed 20 Nov. 2013).

[534] Die Presse (25.07.2012): Harte Zeiten für Schuldner http://diepresse.com/home/wirtschaft/boerse/1270763/Harte-Zeiten-fur-Schuldner?from=suche.intern.portal (accessed 20 Nov. 2013).

[535] Die Presse.com (16.03.2011): Schwarze Listen: "Sie sind leider nicht kreditwürdig", http://diepresse.com/home/meingeld/verbraucher/642381/Schwarze-Listen_Sie-sind-leider-nicht-kreditwuerdig (accessed 20 Nov. 2013).

[536] DiePresse.com (07.07.2009): Auf die Banken kommt der nächste Orkan zu, http://diepresse.com/home/meinung/kommentare/leitartikel/493031/Auf-die-Banken-kommt-der-naechste-Orkan-zu?from=suche.intern.portal (accessed 10 Nov. 2013).

Die Presse (10/2009): Banks alleviate their credit policy partially[537]

Housing is easier to finance. For the fourth quarter some banks expect to loosen their standards somewhat, 90 percent of the banks surveyed at least do not want to tighten them.

Die Presse (05/2009): Loans: Credit customers are likely to experience more stringent times[538]

Loan losses in Austria doubled, outstanding amounts collected harder.

Die Presse (08/2008): Data protection: "Debt free", just like that[539]

Estimated 150,000 people are regarded as insolvent in Austria. The possible deletion from credit databases brings lenders in a quandary.

Krone (01/2008): You want a loan? This is what the bank looks at[540]

Especially in the case of major purchases, it can happen that they can not be paid out of pocket: a car, new furniture or even a house? No matter funding must be found. But who gets any money from the bank? And under what conditions? Find out what you should consider in order to appear creditworthy.

---

[537] Die Presse (28.10.2009): Banken lockern teilweise ihre Kreditpolitik http://diepresse.com/home/wirtschaft/boerse/517949/Banken-lockern-teilweise-ihre-Kreditpolitik?from=suche.intern.portal (accessed 20 Nov. 2013).

[538] Die Presse (19.05.2009): Darlehen: Kreditkunden dürften strengere Zeiten erleben http://diepresse.com/home/wirtschaft/economist/480691/Darlehen_Kreditkunden-durften-strengere-Zeiten-erleben?from=suche.intern.portal (accessed 20 Nov. 2013).

[539] DiePresse.com (06.08.2008): Datenschutz: „Schuldenfrei“, einfach so,

http://diepresse.com/home/wirtschaft/economist/404298/Datenschutz_Schuldenfrei-einfach-so?from=suche.intern.portal

(accessed 10 Nov. 2013).

[540] Krone.at (25.01.2008): Du willst einen Kredit? Darauf schaut die Bank, http://www.krone.at/Oesterreich/Du_willst_einen_Kredit_Darauf_schaut_die_Bank-Kreditwuerdig-Story-89626 (accessed 20 Nov. 2013).

9 Empirical Notes: Methods Used and Field Contacts

- Informal guideline based face-to-face research conversations (interviews) with service staff in Austrian banks (Bank Austria, Erste Bank);
- Informal guideline based research phone calls (interviews) with service staff of Austrian banks (Bank Austria, Erste Bank);
- Informal guideline based face-to-face research conversation (interview) with financial market authority (FMA) employee; several e-mail contacts;
- Research phone call (interview) with 'quintessenz';
- Library research (University of Vienna) and online literature research;
- (informal) research conversations with concerned credit users;
- Subject-access-requests (self-disclosure) and research phone calls at KSV and CRIF;
- Media analysis: newspaper archive research; sample: DiePresse.com, derStandard.at, wirtschaftsblatt.at; (used Keywords: credit, creditworthiness, credit scoring, credit rating, creditmanagement);

10 References

Basel Committee on Banking Supervision (2004): *International Convergence of Capital Measurement and Capital Standards – A Revised Framework*; Bank for International Settlements, Press & Communications, CH-4002 Basel, Switzerland, ISBN: 92-9197-669-5

Bornett, Walter; Bruckner, Bernulf; Hammerschmid, Hans, Masopust, Herbert (2006): *Rating-Kennzahlen. berechnen-analysieren-verbessern.* Wirtschaftskammer Österreich, Abteilung für Finanz- und Handelspolitik; WIFI Unternehmerservice; Kammer für Wirtschaftstreuhänder. AV + Astoria Druckzentrum GmbH.

Butschek, Christian (2008): *Basel II, Zinsklauseln und Offenlegung des Rating,* in: Bank-Archiv, Zeitschrift für das gesamte Bank- und Börsenwesen (ÖBA), 56. Jahrgang, S. 240 - 248.

Die Presse (07.10.2013): *Die (fast) vergessene Datenaffäre*, URL: http://diepresse.com/home/panorama/oesterreich/1461401/Die-fast-vergessene-Datenaffaere?_vl_backlink=/home/index.do (Abgerufen am 07.10.2013).

Hayden, Evelyn (2003): *Are Credit Scoring Models Sensitive With Respect to Default Definitions? Evidence* from the Austrian Market, University of Vienna, Department of Business Administration Chair of Banking and Finance, Vienna.

Helmreich, S. (2008): *Validierung von (Retail)Ratingmodellen unter dem Blickwinkel von Basel II,* D.M.S., Studie gesperrt.

Knyrim, Rainer (2008): *Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?;* in: ecolex Zeitschrift für Wirtschaftsrecht, S. 1060-1062.

Krenn, Michael; Zeger, Hans G. (2009): *Datenschutzbestimmungen zur "Auskunft über die Kreditwürdigkeit"*, in: Bauer, Lukas; Reimer, Sebastian (Hg.) Handbuch Datenschutzrecht, Wien, facultas.wuv, S. 533-549.

Strobl, Gerhard; Hahn, Friedrich (2010): *Lehrgang für Finanzmarktaufseherinnen und -aufseher, Modul 1.07, Einführung Kreditgeschäft.* Aufsichtsakademie der Finanzmarktaufsichtsbehörde und Österreichischen Nationalbank, Skriptum, September/Oktober 2010.

Thonabauer, Günther; Nösslinger, Barbara; Datschetzky, Doris; Kuo, Yi-Der; Tscherteu, Alexander; Hudetz, Thomas; Hauser-Rethaller, Ursula; Buchegger, Peter (2004): *Guidelines on Credit Risk Management – Rating Models and Validation.* Published by: Oesterreichische Nationalbank (OeNB), Financial Market Authority (FMA), Vienna.

Thonabauer, Günther; Nösslinger, Barbara; Buchelt, Roman; Unteregger, Stefan; Fend, Wolfgang; Zwizlo, Radoslaw; Lutz, Johannes; Buchegger, Peter (2006): *Guidelines on Operational Risk Management*; Published by: Oesterreichische Nationalbank (OeNB) and Austrian Financial Market Authority (FMA), Vienna.

Zeger, Hans G. ; Krenn, Michael (2007): *Datenschutzpraxis von Wirtschaftsauskunfstdiensten*, in Reifenstein/Blaschek (Hg.) Konsumentenpolitisches Jahrbuch 2005-2006, 283-360, Verlag Österreich 2007.

IRISS WP3

Credit scoring as a form of surveillance in Hungary

Final draft

Ivan Szekely and Beatrix Vissy

15 December 2013

The history of credit scoring, its present practice, as well as public attitudes towards this form of checking one's financial status, clearly reflect the recent political and social history of the country. As one of the countries of the Soviet Block, Hungary did not introduce a full scale market economy until the fundamental political changes of 1989. The majority of the population was not prepared for the economic transition, had no information about capitalist methods in market economy, nor experience in managing one's financial matters in the new economic environment. Although a new generation has grown up since the collapse of the old political system the members of which are more familiar with economic matters, especially the means and methods of managing their finances, a significant part of the population does not even understand the basic notions of the credit system. This could be observed when in the mid-2000s masses of people took financial loans from commercial banks in western currencies, mostly in Swiss franks, although Hungary is not a member of the euro zone even today, and the risks of adverse changes in the foreign exchange rate were high. These people, a part of whom took the credit for buying fashionable consumer goods, such as home movie screens because the credit seemed cheap, belong today to the mass of bad debtors and have difficulties in paying back the loan. Although the present government launched a retroactive campaign against the commercial banks, alleging that the banks had deliberately deceived their customers, the magnitude of taking

such credits indicates the lack of knowledge and the inability of understanding the risks in finances in large segments of the population.[541]

The revealing of surveillance practices of the old political regime, and in particular the surveillance practices of the security services during the turbulent period of the political transformation, gained high publicity and became an important element of public discourses.[542] However, these practices were represented in people's mind as activities of secret agents, tapping of phones or later installing of CCTV cameras, rather than analyzing of people's financial status or their personal data in general. A comprehensive press analysis revealed that in the period 1987-1990 despite the large number of press articles on privacy- and surveillance-related matters, most of these articles focused on the surveillance of people as *politicians,* not as *private individuals*.[543] At present, credit scoring in general is not understood as a form of surveillance, not only because of the high threshold of abstraction[544] but also because people tend to regard credit scoring as part of the financial system and not as an activity revealing information about their private life.

These antecedents, the low level of knowledge and awareness, and the missing link in people's mind between the new methods of market economy and surveillance jointly constitute the environment, which determines people's attitudes towards credit scoring, and indirectly, the conduct of financial institutions and credit reporting agencies.

---

[541] One could also observe here a sign of the long-standing paternalistic traditions according to which you can easily take risk because if you get in trouble, the state or the ruling regime will help you anyhow.

[542] The "Budapest Watergate" or "Duna-gate" scandal of 1990 when activists clandestinely filmed the documents proving that the secret services had continued keeping the new political leaders and activists under surveillance, played an important part of the political changes, see Szekely, Ivan, "Hungary", in James B. Rule and Graham Greenleaf (eds.), Global Privacy Protection: The First Generation, Edward Elgar Publishing Ltd., 2008.

[543] "Aspects of Privacy and Informational Autonomy in the Press", Hungarian Institute for Mass Communication Research, 1991. [in Hungarian]

[544] See Szekely, Ivan, "Changing attitudes in a changing society? Information privacy in Hungary 1989–2006", in Elia Zureik et al. (eds.), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons,* McGill-Queen's University Press, Montreal & Kingston, London, Ithaca 2010, pp. 150–170.

1. The evolution of credit scoring in Hungary

The only antecedent of present-day credit scoring in the interwar period which deserves attention was the practice of the so-called credit information letters. Banks were sending letters directly to the clients of the borrower, asking information about the borrower's financial standing and debts.[545] Although the clients had no legal responsibility regarding the provided information, at that time the morals in business matters were at a higher level than today.[546]

This was followed by four decades of centralized planned economy, which contained limited forms of market economy on a small scale, primarily since the 70s, however, banking demands of the citizens were satisfied mostly by a single financial institution, the National Savings Bank (OTP) the credit policy of which was shaped by central financial politics.

Although the restructuring of the financial system, especially of the bank sector, started already before the political transition of 1989, the critical conditions of the economy did not allow a market for loans until the mid-1990s. That time, the slow increase in the volume of consumer lending was influenced by several factors: the process of economic liberalization and privatization of state-owned enterprises, the macroeconomic stabilization program (both fiscal and monetary measures), the establishment of prudential regulation (on minimum capital standards, liquidity ratios, the concept of solvency and capital adequacy etc.) and further regulatory measures (e.g. on mortgage banks and mortgage bonds), the strengthening of property rights protection (bankruptcy laws, contractual discipline enforced by courts).[547] Until 2001, however, the total of financial loans taken by citizens from commercial banks was very low, altogether 5% of the GDP, while at that time this rate was

[545] Schack, Béla, *Révai Kereskedelmi, Pénzugyi és Ipari Lexikona* [Revai's Commercial, Financial and Industrial Lexicon], 1930.
[546] Vértesy, László, "A pénzugyi intézmények finanszírozási tevékenységének jogi szabályozása Magyarországon" [Legal regulation of the financing activities of financial institutions in Hungary], PhD dissertation, manuscript, Budapest, 2008, p. 307.
[547] For more details on the development of pillars of the financial sector development in Hungary and the CEE region in English see: Lajos Bokros, Alexander Fleming, Cari Votava (eds.): *Financial Transition in Europe and Central Asia: Challenges of the New Decade,* The World Bank, Washington D. C., Washington, 2001.

around 46% of the GDP in the member states of the European Union.[548] In 2001 the introduction of state subsidized home loans resulted in a sharp increase in the financial loans of the population.

Until the global financial crisis the regulation of the activities of financial institutions was rather liberal, with no significant regulatory restrictions on credit scoring. The Parliament enacted a general provision already in 1993 that financial institutions providing loans are obliged to obtain information about the credit standing of the borrowers and their guarantors. [549] Even the comprehensive legal reform of the financial sector, which took place in 1996, did not introduce new provisions regarding the checks on the borrowers' financial status.

Act CXII of 1996 on Credit Institutions and Financial Enterprises (hereinafter: CIFE Act), which is the most important act in the area of loan market and which is applicable to all financial services provided in the territory of Hungary, provided only for certain general rules on credit rating as part of the prescriptions concerning the requirements of prudent operation of credit institutions. For almost two decades scoring attributes were regulated only in the internal regulations of financial institutions, the preparation of which are stipulated in the CIFE Act: "Financial institutions (…) must adopt internal rules and regulations, subject to approval by the board of directors, to provide sufficient facilities to establish the substantiality and transparency of placements and exposures as well as to control the assessment of risks and to mitigate them." [Section 77 CIFE Act] Other general provisions include that "Prior to deciding on a placement, the credit institution must ascertain the existence, value and enforceability of the necessary collaterals and securities. The documents substantiating such decision must be attached to the contract for the deal." [Section 78 of CIFE Act] Consequently, the credit scoring practices has been developed by the commercial banks individually, constituting sensitive business secrets.

[548] Data published by the Central Statistical Office

[549] Act No. CXII of 1993 on the amendment to Act No. LXIX of 1991 on financial institutions and financial institutional activities, Section 15.

Although the present legal regulation still provides significant room for self-regulation, the laws enacted as a reaction to the global financial crisis restricted the independence of financial institutions in the area of credit rating. The most significant regulatory change regarding credit scoring was the Act CLXII of 2009 on retail lending, and its implementing Government Decree No. 361/2009 (XII. 30). The aim of the Act was to achieve profound changes in the practice of retail lending with a special focus on consumer protection in order to meet the expectations of the European Union declared in the Consumer Credit Directive 2008/48/EC. These statutes contain specific rules on credit rating for ensuring the correct and reliable information on the consumers.

The Government Decree is applicable to credit agreements (also financial leasing arrangements) concluded with natural persons, including real estate and car financing. The decree introduced strict rules applicable to financial institutions in terms of their internal guidelines and required thorough scrutiny of creditworthiness. Lenders are not allowed to offer loans to the borrowers solely on the basis of credit risk contributions, they are obliged to check the financial standing of natural person applicants in each credit arrangement procedure. The checks shall be based on the personal or family income of the applicants. [Section 3 (1)-(2), Act CLXII of 2009]. The result of these checks is the individual credit limit for each borrower, defined in the local currency (Hungarian Forint), representing the maximum monthly paying ability of the borrower. Banks are only allowed to provide loans the monthly payment of which does not exceed this limit.

2. The evolution of the central debtor list

Commercial banks had raised the idea of establishing a central debtor list several times in the early 1990s. However, at that time there was no commonly agreed opinion on the

concept of such a register even inside the financial sector. Banks were not interested in sharing confidential information about their lending policy with their competitors, and the legal framework was not favorable either for establishing such a credit information system. The confidentiality of banking data was protected by regulation on bank secrets and business secrets, while the autonomy of the natural person customers of commercial banks was guaranteed by their right to informational self-determination. Consequently, a comprehensive legal framework had to be worked out, within the limits of the general legal system established after the change of the political system.

The first step in working out such a legal framework was an amendment to the then existing act on financial institutions[550] in October 1993. This amendment lifted some of the restrictions on forwarding information which constitutes a bank secret. According to the new provisions, the following shall not constitute violation of bank secrets: provision of information on the name (description) and number of a client's money circulation account; provision of general information containing no details, on the solvency of a client, unless such provision of information is prohibited by the client with an express stipulation in the contract concluded with the financial institution; provision of information for the central credit information system of financial institutions in respect of debtors, established and operated by financial institutions, and provision of information from the above system for a financial institution [Section 47 (1), b)–d)]

On this legal basis eight leading commercial banks in Hungary established a joint venture called Inter-Bank Information Service Corp. (BISZ), which started to operate the Inter-Bank Debtor and Credit Information System in June 1995. While in Western European countries the central banks initiated the establishing of such registries, in Hungary the commercial banks took this role. Soon after the launch of registry smaller banks have also joined the system, and by 1996 virtually the whole financial loan market entered the Inter-Bank Debtor

[550] Act no. LXIX of 1991 on Financial Institutions and Financial Institutional Activities

and Credit Information System. In 1998 the new Banking Act made it obligatory for all financial institutions offering loans to join the system.

However, the legal basis provided by the 1993 amendment did not allow the registration of natural persons in the registry, for reasons of data protection rights. At that time financial loans to natural persons were offered predominantly by a single financial institution, the National Savings Bank, which had a monopoly in handling citizens' financial matters before the political changes. In the second half of the 1990s the expansion of demands for a market of credit institutions made it necessary to include provisions regulating the use of credit information on natural persons, too. This was achieved in 1998 when an amendment of the new CIFE Act made it possible to enter the data of those individual debtors whose debt exceeds the minimum wage and who are in default for more than 90 days.

Thus the first period of the Inter-Bank Debtor and Credit Information System – later renamed as Central Credit Information System – had been functioning solely as a "negative" debtor list, until 2011. In this period the Inter-Bank Information Service Corp. became a sole-owner institution (owned by the GIRO Clearing House Corp.) in 2003, and in 2005 a comprehensive customer protection reform took place, as a result of the high number of customer complaints submitted to the Hungarian Financial Supervisory Authority and the Parliamentary Commissioner for Data Protection and Freedom of Information. The majority of the complaints revealed that the customers had not been sufficiently informed about the existence of the debtor list, they could realize their registration in the list only when their loan applications were rejected; it was difficult to have access to one's own data in the list and to correct inaccurate data or delete the data if entered unlawfully, furthermore the customers had no efficient legal remedies in matters related to the central debtor list.

In 2002, the Hungarian Banking Association initiated consultation with the government on the introduction of the positive debtor list model. However, the subsequent data protection

commissioners had managed to block these attempts to broaden the credit reporting system until 2011. In 2002, at a conference organized jointly with the Ministry of Finance, the Ministry of Justice, the Hungarian Banking Association, the Hungarian National Bank, and the Financial Supervisory Authority, the Commissioner raised his voice against "setting up a positive debtor reporting system that would not only keep central records of any debt over the minimum wage in default for more than 90 days, but also the entire data content of every credit and loan contract signed in the country". The Commissioner emphasized that the proposed regulation did not meet the criteria for restricting the right to data protection, including those of necessity, proportionality and suitability to achieve the declared purpose. The Commissioner cited his French colleague, who questioned the efficacy of the positive listing and cautioned that "it provided wider loopholes for violating the principle of purposefulness, because the large number and broad range of information contained in such lists presented a serious temptation of using the data for divergent purposes."[551]

Finally, in October 2011 the Parliament passed a new act on the Central Credit Information System that has re-regulated and expanded the scope of the credit information system. The project was managed by the Hungarian Banking Association, the BISZ Corporation and financial stakeholders. The lawmakers introduced the mandatory registration of positive credit data on natural persons. However, while no statement of consent of data subjects is required for access to negative information, registration in the positive debtor list makes access by financial institutions dependent on the opt-in based consent of the customer concerned. Customers should give such consent in each case, otherwise their bank will only receive information on past events of credit default and fraud, without any positive credit data, for the purpose of assessing credit applications.

[551] Annual report of the Parliamentary Commissioner for Data Protection and Freedom of Information, 2002., Budapest, 2003, p. 38. Available at https://81.183.229.204:51111/dpc/index.php?menu=reports/2002/II/A/7

The central credit information system, containing both the negative debtor list and the positive debtor list, became a major component of the credit scoring practice of the banks and other credit institutions. According to the statistical data published by the BISZ Corporation, in 2002 data of credit contracts of 155,000 individuals were stored in the system, while this number has recently reached 4.8 million (in a country of approximately 10 million inhabitants).

3. Changes in the policy of credit institutions[552]

In recent years there has been a fundamental change in credit policy of financial institutions, due to two main reasons: first, the global (and national) financial crisis increased the risks of bad debts, and second, the economic and financial politics of the government became erratic and unpredictable. In this situation the trust in the state as a financial resource has significantly decreased, thus an important type of guarantee (for example, a successful grant application for financial support in a government program) which traditionally belonged to the best ones, has lost its weight in credit scoring. The factors taken into consideration have diversified, extending to the debtor's capital and valuables, his/her personal character, or credit history. It is a growing practice that banks require invoices of public services as an additional check on the debtor's financial standing, then double check the invoices with the public utilities, and set up a black list of forged documents and their owners.

Interestingly, preferential treatment of clients with a good credit history and a long-standing relationship with the credit institutions has not become widespread in the practice of commercial banks. Instead, the weight of subjective elements in credit decisions increased, thereby requiring more credit scoring expertise and human participation.

[552] This section is based on an interview conducted with an expert consultant who has been doing consultancy in credit scoring and other the areas of the financial sector in Hungary.

An important activity of the civil organizations established for the representation of debtors is to start joint lawsuits against banks on the grounds that the banks had deceived their clients when offering loans in foreign currencies. However, legal actions started by individual clients against credit institutions – in any matter – often end with out of court agreements.

5. Resilience of data subjects towards credit scoring

Since natural person clients of credit institutions generally regard credit scoring as part of a financial procedure and not as processing their personal data – and especially not as a form of surveillance – their resilience, if any, is directed primarily towards the financial procedure. This is understandable because personal data in everyday practice rarely appear as abstract notions, rather as part of a customer relationship of a financial procedure. Most people realize that the processing of their personal data within a credit relationship with a financial institution may have an impact on their private life when they happen to default of paying back the loan. The following sections of this report on the judicial practice, the cases of the data protection supervisory authority and on how credit scoring issues are presented in the media, will support these observations from different aspects.[553]

The registration of credit data in the central credit information system is mandatory, and so is the process of credit rating by credit institutions, therefore there is no way to avoid this procedure, even if it is not visible for the client. Two ways of doctoring the system, as forms of resilience, can be experienced, mostly through informal sources: in smaller towns where potential applicants may personally know those employed by the local credit institutions, the applicants ask their acquaintances to circumvent the checks on their financial standing if the result of these checks may have an adverse impact on their chances in getting the loan. The

[553] It deserves noting that the financial sector in general, and credit institutions in particular, have also developed a significant level of resilience towards legislative changes and the positions of the data protection supervisory authority. Financial institutions in the last two decades managed to retain their positions and follow the interests and logic of collecting as much information about their clients as possible.

other way of tricking the system is to ask friends or acquaintances to falsely testify on the applicant's creditworthiness, or to produce false guarantees of his financial standing.

5. Judicial practice

After having reviewed the judgments of the last six years that were published in the Compendium of Court Decisions of Hungary,[554] we concluded that Hungarian citizens exhibit a low level of demand for launching lawsuits against credit institutions solely for the reason that their personal data were processed in a controversial way. The reluctance on the part of debtors to file lawsuits against financial institutions which possibly violated their right to privacy is clearly demonstrated by the quantitative and qualitative findings of our research. As regards the period of jurisdiction between 2007 and 2013 that we took under scrutiny, we identified only 48 cases having some connections with processing of personal data for credit-scoring purposes. Only 32 of these lawsuits could be considered as relevant from our point of view since the rest of the cases did not reveal any objection on the plaintiff's side to this form of surveillance (e.g. legal debates among financial institutions, questions of legal interpretation) or had to be left out for other reasons (e.g. lawsuits filed by legal persons).

The cases were analyzed with one question in mind: what was the trigger for litigation? *Can the mere fact of being kept under this objectionable type of surveillance by credit institutions be deemed as the trigger for filing a lawsuit, or only certain negative consequences of this fact for the plaintiff's private or business life can be considered as such?*

What we found was that none of the examined cases questioned whether the range and amounts of personal data to be processed in the credit sector was necessary and

[554] Since 2007, the Hungarian State has been obliged by law to operate a public judgement database that makes a wide range of judicial decisions accessible in a digital and anonymized form to anyone without identification or charge. The database is available at the official website of the ordinary courts of Hungary: http://www.birosag.hu/ugyfelkapcsolati-portal/anonim-hatarozatok-tara

proportional or whether the data management complied with the principles of purpose finality and purpose limitation. The decisions and their justifications in the 32 lawsuits revolved solely around the plaintiffs' concerns about the transmission of their credit records to the Central Credit Information System and its various negative consequences (such as rejected credit applications, aborted sales contracts or reduced income).

This finding suggests, as stated above, that as long as the processing of personal data *seems* to converge on the customers' interests, customers do not pay enough attention to the form and intensity of the surveillance they formally consent to. Thus, on the basis of the accessible judicial documentation in this area, resistance can only be discovered in attitudes of those people who happen to default of paying back the loan in time.

The vast majority of cases were launched with courts for the deletion of credit records from the system and for compensation for damages. The majority of the lawsuits in this area concluded in favour of the information service provider, i.e. organizations of the bank sector, because no violation of legal rules was established. Nevertheless, 9 of the 32 analyzed cases were filed as a libel case.[555] This means that several plaintiffs argued that registration without legal basis in the Central Credit Information System definitely involves a defamatory character regarding the data subject. As regards the compensation for damages to individuals, it deserves noting that the Hungarian courts generally[556] decide in this matter on the basis of the principle of strict liability, regardless of any actual damage incurred or regardless of the size of such damages, taking it as a natural fact that being registered in the Central Credit Information System entails disadvantages. [557]

[555] Cases 24198/22.P.26.317/2008/5; 23356/27.P.20.578/2007/17; 26107/(…)P(…)2008/10; 29287/…P…2010/14; 3400/19.P.23.063/2006/11; 37048/32.G.42.024/2009/27; 61432/2.Pf.21.767/2010, 62170/2.Pf.21.382/2007/5; 63626/4.Pf.20.857/2008/4.
[556] For one exception that we found see: 26107/…P…2008/10.
[557] Report on Activities of the Hungarian Banking Association – 1st Quarter 2011, p. 15. Available at http://www.bankszovetseg.hu/wp-content/uploads/2012/09/2011-1st-Quarter.pdf.

6. Cases from the data protection supervisory authority

The activity of the data protection supervisory authority is a significant indicator of the relevant issues in the respective sector-specific data processing areas, including the data processing of financial institutions – the wider environment of credit scoring. As mentioned elsewhere, from 1995 to 2011 the institution of the Parliamentary Commissioner for Data Protection and Freedom of Information fulfilled the role of the independent supervisor. The institution was dissolved in 2011 and replaced by a newly established government authority, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH). The authors of this report initiated an interview with an expert from NAIH, who had been serving in the office of the Commissioner before joining the new authority, and has been responsible in both organisations for cases involving data protection issues at financial institutions. Although the authors initiated a professional discussion, not an official interview, the expert politely declined from the discussion. Therefore the following overview is based on the series of annual reports of the Commissioner, which, besides presenting individual cases, shed light on the shifts in the composition of complaints regarding financial institutions in general and credit scoring in particular.

In the first three years of the Commissioner's activity (1995–1997) the typical cases in the area of financial institutions were focusing on what kind of personal data was the financial institution entitled to in certain types of banking transactions. The credit scoring landscape significantly changed with the setting up of the central credit information network, which was extended to include private individuals as of 1 January 1998. The draft legislation was evaluated by Commissioner. Considering the purpose of the network, namely to screen out habitual defaulters, the Commissioner saw no justification for a broad authorisation that

would allow banks to collect data indiscriminately from those who default on their payments and those who make them regularly on time.[558]

In the early 2000s the number complaints against the data processing practices of financial institutions multiplied. In his 2001 report the Commissioner observed that "Clients are sensitive to the fate of their data in the financial sector, and often think that the hunger of banks for personal data is exaggerated."[559] As the Commissioner explained, it followed from the principle of finality in processing data that banks were not authorized to demand information from their clients in excess of what was strictly necessary to achieve the purpose of the processing. By placing a loan, banks assumed a certain credit risk, which they sought to minimize by collecting data about their clients. The Commissioner, however, explained that it followed from the principle of finality in processing data that banks were not authorized to demand information from their clients in excess of what was strictly necessary to achieve the purpose of the processing.

Another significant observation of the Commissioner was that banks kept the data of rejected clients on file without authorization by law, for purposes of compiling statistics for product development. In this matter the President of the Financial Supervisory Authority shared the Commissioner's standpoint and proclaimed that keeping and using such data ran counter to the principle of finality enshrined in the data protection act.[560]

Act XV of 2003 on the Prevention of Money Laundering set the liability of financial service providers to identify their clients by requiring them to verify the client's (or his authorized

[558] The first three years of the Parliamentary Commissioner for Data Protection and Freedom of Information, Budapest, 1998, p. 96. Available at https://81.183.229.204:51111/dpc/index.php?menu=reports/1995/VI/1
[559] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2001, Budapest, 2002, p. 57. Available at https://81.183.229.204:51111/dpc/index.php?menu=reports/2001/I/A/6
[560] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2002, Budapest, 2003, p. 40. Available at https://81.183.229.204:51111/dpc/index.php?menu=reports/2002/II/A/7

representative's) proof of identity and to record a certain set of data in writing. The Commissioner learned that a large residential bank had sent out letters to its clients, calling on them to supply the required data, and this elicited objections from a number of clients. The Commissioner found that some of the data sought on the form designed to fulfil the reporting obligation did not correlate with the legal obligation and the clients had not been informed about the purpose of processing these data. The Commissioner instructed the institution not to accept any more such incoming statements, and to delete the objected data from both the forms that have already been received and from the electronic database generated from them. The executive of the bank pledged to revise the records as instructed, and to properly inform the clients about the purpose of the processing.[561]

In a complaint of 2003 an inquirer called the credit information line of a bank, where the administrator said that credit conditions could be communicated only after having provided the inquirer's personal data. The Commissioner stated that only in case of preliminary credit scoring could the bank ask for personal data of the inquirer (not in case of seeking general information only), and after having learnt the result of the preliminary credit scoring the data subject might decide over the keeping or deleting of her personal data in the data processing system of the bank.[562]

In the year 2004 several complaints were submitted to the Commissioner objecting to the practice that the central credit information system contained their data, although they acted only as guarantors, not debtors. The Commissioner instructed the company operating the system to delete such data and informed the banks about the unlawful nature of such forwarding of data of guarantors. In its reply the company stated that the data subjects

[561] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2003, Budapest, 2004, p. 31. Available at https://81.183.229.204:51111/dpc/index.php?menu=reports/2003/I/A/11
[562] Case 368/A/2003

registered in the central credit information system were not distinguished according to their role as debtor or guarantor, consequently such deletion of data was not feasible.[563]

By 2005 the 40 percent of the cases regarding the data processing practices of financial service providers contained complaints against the operation of the central credit information system.[564] However, after the entry into force of the new legal provisions regulating the system, making the operation of the system more user-friendly, this number dropped to 1-2 percent, and the complaints submitted in this matter proved to be unfounded. This shift clearly shows the interdependence of the legal regulation and the Commissioner's quasi case law.

In 2008 the Commissioner did not find unlawful the collecting of socio-demographic data for credit scoring purposes in certain credit constructions. However, the Commissioner objected to the practice of a bank, which used the tax identification number to “decode” the birth date of the data subject in commodity credit applications.[565]

By the end of the decade debt collection became the segment in the banking industry mostly criticized by citizens. The Commissioner stated several times that collecting information about the debtor from neighbours or employers did not only infringe the data protection rights of the debtor but those of the neighbours, too.[566]

In the 2002 annual report of NAIH[567] (the first annual report of the authority) there is no mention about cases relating to credit scoring or processing of personal data of debtors.

[563] Case 1305/K/2004
[564] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2005, Budapest, 2006, p. 50. Available at https://81.183.229.204:51111/dpc/index.php?menu=reports/2005/II/A/8
[565] Case 101/P/2008
[566] Cases 1398/P/2009, 2184/P/2009
[567] http://naih.hu/files/Annual-report_NAIH_2012_EN_FINAL1.pdf

7. Credit scoring in the media

Individual financial loans, in particular the problematic foreign currency loans are popular themes in Hungarian media since the mid-2000s. These news and articles, however, concentrate mostly on the general responsibilities of banks, the administrative measures introduced by the government, or individual life circumstances of bad debtors, their street demonstrations – credit scoring as such rarely appears in itself in the media. The number of cases in direct or indirect connection with credit scoring practices reported in the media is limited. One part of these reported cases deal with the general data protection aspects of data processing practices in financial institutions only, but even these cases may have some relevance in the credit scoring process.

The typical examples of media coverage presented below have been collected on the basis of the cases reported in the biggest circulation economic weekly[568] and in national daily newspapers since the early 2000s.

A recurring issue in data protection cases in financial institutions is the photocopying of personal identification documents, which is a widespread practice of the financial institutions when receiving credit requests from individuals. Banks and other financial institutions, according to their explanation, copy these documents in order to reduce the number of frauds, and sometimes only because of their administrative traditions.[569] However, according to the laws in force, such institutions and other service providers are allowed to record only

[568] *Heti Vilaggazdasag* [Weekly World Economy] or *HVG*.
[569] Photocopying of identifying documents containing photographs may indirectly provide opportunities for unlawful discrimination: if the decision-maker, who has not met the requester personally, decides on the basis of the photograph that the requester is risky or simply not wanted, because of his look, clothing or skin color, the credit (or other bank services) will not be granted to the requester, even if he or she meets all requirements. Naturally it is almost impossible to demonstrate this practice, but it is not unknown in informal financial circles.

certain personal data, as well as the serial number of identifying documents containing these data, but photocopying the identifying documents themselves is not allowed.

A customer wanted to open a bank account in a branch office of Raiffeisen Bank, but since he did not consent to the photocopying of his personal identity documents, the bank was not willing to open the account for him. The customer presented his documents to the bank employee to no effect, he was obliged to fill in a separate form with all the data included in his identifying document, what he denied to do. He argued that the same data had already been in the possession of the bank in connection with his earlier bank account. The customer turned to the Financial Supervisory Authority, which affirmed that banks had no right to stipulate such conditions for providing of services. Nevertheless, the customer was able to open the account only when he filled in the unlawful form. He then demanded compensation for damages from the bank; the bank refused his demand, and in this matter the supervisory authority did not support his claims either.[570]

In a similar case the customer started a court action, which finally reached the Supreme Court. The customer deposited an amount of about thousand euros to his own bank account in CIB Bank when the bank employees obliged him to present his identifying data. The customer found this practice unlawful and sued the bank. In its decision the court of first instance rejected his claim, referring to the act on the prevention of money laundering, the provisions of which allow banks to process personal data in case of suspicion of money laundering. In this case, however, there was no such suspicion, as the bank admitted, consequently the final decision of the Supreme Court stated that no such legal provisions existed which allowed the banks to process the personal data of those customers who deposit money to their own accounts, in the absence of the customers' consent.[571]

[570] Andrea Salgó, “Minimax infók” [Minimax infos], *HVG* 2010/13 (03 April), p. 98.
[571] “Adatvedelmi precedens” [Data protection precedent], *HVG* 2010/10 13 March, p. 12.

The Parliamentary Commissioner for Data Protection and Freedom of Information – until the dissolving of his office – investigated a number of cases relating to the practice of photocopying personal identification documents as well as general anomalies of data processing in banks.[572] From time to time the media reported about the Commissioner's positions and recommendations in this area. Among others, the biggest circulation national daily in Hungary, *Népszabadság* – quoting the communiqué of the national news agency – reported on the investigation of the Commissioner at Citibank, in which the Commissioner determined that Citibank demanded the photocopying of the personal identification card, the tax identification card and the social security card of the customers, justifying this practice by the high risks of fraud, and consequently rejected the credit applications of those who objected to this practice. According to the information of the Commissioner, the bank retained for six months the personal data of even those customers, whose applications had been rejected, arguing that it needed these data for preparing internal statistics in order to develop the bank's products. The Commissioner requested access to the credit scoring regulation of Citibank but the bank unlawfully refused the Commissioner's demand on grounds of business secrecy.[573]

It was *Népszabadság* again, which reported about a case in which a student did not get a student loan because he had no consented to the forwarding of his data to a specific bank – Postabank – in order to open an account for him there. The irony of the case was that although the student did not get the loan, his data were forwarded and an account had been opened in his name in Postabank. The spokesman of the Student Loan Center – supposedly

[572] See the series of annual reports of the Commissioner: *Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information, 1995/96–2010,* published by the Office of the Parliamentary Commissioner for Data Protection and Freedom of Information, Budapest.
[573] "Torvenyserto banki ugyintezes" [Unlawful banking administration], *Nepszabadsag,* 08 February 2000, p. 25.

as a consequence of adverse publicity in the media – apologized for mistakenly opening the account.[574]

Another type of cases reported in the media contains stories in which the customer suffered damages or loss of profit because he was registered in the bad debtors list for ill-founded reasons, or with incorrect data.

A married couple sued the OTP Bank (the biggest commercial bank, which had been operating before the change of the political system as a monopolistic, state-owned commercial bank in Hungary) for a compensation of hundred million Forints (about three hundred thousand euros) because the bank registered them on the blacklist of debtors. The couple lost the government subsidy on their home loan and all other opportunities of getting loans because of being registered on the blacklist. Although the bank later acknowledged the maladministration, this did not help the couple since OTP Bank had already forwarded their data to the central debtors list.[575]

In an article in 2006 *HVG* provided an overview of cases where the banks terminated the credit agreements. Although the explanation of the terminations generally complied with the law, one part of the debtors started court actions against the creditors because they found the termination of the contract unjust. This was the case in which a leased car had been stolen and while the debtor was debating with the insurance company, his leasing contract was terminated.[576]

In another article the economic weekly reported on consequences of being erroneously registered on the blacklist of debtors. In one case Postabank miscalculated the amount of

[574] "Diakhitel: serult az adatvedelem" [Student loan: data protection infringed] *Nepszabadsag*, 13 November 2001, p. 6.
[575] Agnes Gyenis, "Az a fekete folt" [That black spot] *HVG* 2007/14, 07 April, pp. 107-108.
[576] Emilia Papp, "Eros lista" [Hot list], *HVG* 2006/05, 04 February, pp. 92-93.

the repayment instalments, and while the debtor, in good faith, was paying the original instalments as stipulated in the contract, the difference between the original and the wrongly calculated debt repayment reached the level defined by the law, the bank registered the debtor on the list. Later the bank admitted its error and deleted the debtor from the list. Another aggrieved party got to the blacklist because of a debt of 28 thousand Forints (less than 100 euro), again resulting from the bank's fault. In 2004 about hundred customers turned to the Financial Supervisory Authority, either because their names were registered on the list unlawfully, or because they found the consequences of being on the blacklist exaggerated.[577]

A national daily published an article about the blacklist victims who did not know that they had become registered on the list, because – according to the legal provisions in force at that time – they did not receive any notification of this fact. The victims complained that they could get their own data on the list only through a complicated process, for a rather high fee. Most banks immediately reject credit applications if they find the applicant's name on the bad debtors list, and the possibly innocent individual has to pay a fee and wait for weeks until s/he is able to determine which bank registered him/her on the list and why.[578] In such cases the debtor has negligible chance of having his damages compensated. The article reports various cases in which the bank admitted its maladministration and removed the customer concerned from the list, however, their damages had not been compensated.[579]

[577] Gergely Fahidi and Agnes Gyenis, “Kiser a mult” [The tracking past], *HVG* 2005/11, 19 March, pp. 66-67.
[578] It should be noted that in 2006 the law regulating the database of bad debtors became more customer-friendly: for example, the bank shall notify the debtor thirty days in advance of registering him on the bad debtors list, and one request per year for the debtor's own data shall be free of charge.
[579] Emilia Papp, “A feketelista aldozatai” [Victims of the blacklist], *Magyar Hirlap,* 13 September 2004, p. 9.

The type of articles which has the most direct connection with credit scoring and surveillance present cases of checking the customer's financial status and other personal data, or collecting further personal data about the customer.

Erste Bank Hungary requested written authorization from its credit applicants according to which the bank would be authorized to collect information about the applicant from anybody, including private individuals, the economic weekly reported. A prospective customer of the bank, upon advice of his lawyer, did not sign the authorization, which would have authorized the bank to check the information submitted by the customer "at any authority, natural or legal person". It would have also authorized the bank to acquire any information on the private bank accounts and business relationships of the customer from authorities, natural or legal persons (for example other banks) being in contractual relationship with the customer. The Commissioner criticized the general authorization, which did not contain concrete definitions of data processors and circumstances. The legal counsel of Erste Bank Hungary explained that the bank needs extensive mandates for checking the validity of the information because a part of the customers submit forged documents, such as personal identification cards, employer's certificates, or statements of account form other banks.[580]

In the same issue the economic weekly published interviews conducted with private detectives and private investigating agencies about the above practice. The respondents confirmed that customers often try to deceive financial institutions, therefore preliminary checking is highly advisable. Nevertheless, according to the responses from the agencies interviewed by *HVG*, most banks ask for external help only when the debtor has already disappeared and it turned out that the contributions could not be easily sold.[581]

8. General conclusions

[580] "Kolcsonvett adatok" [Borrowed data], *HVG* 2004/52-53, 25 December, pp. 166-167.
[581] "Gyakorlati lepesek" [Practical steps], *HVG* 2004/52-53, 25 December, p. 167.

The research conducted in the area of processing personal data in the financial sector in general, an in the course of credit scoring in particular, with special regard to the surveillance character of credit scoring practices and the citizens' resilience towards these practices, reinforced our general impression that neither citizens nor financial institutions – in other words, neither data subjects, nor data controllers – regard the collection, analysing and use of personal data in connection with credit scoring as a separate phenomenon, or a practice which may restrict citizens' fundamental rights or concern their human dignity. Consequently, credit scoring in general is not understood as a form of surveillance, rather as a set of technical measures involving the processing of certain personal data. Therefore the justifiability, finality and proportionality of data processing are almost never contested by the debtors.

This relative disinterest towards the fate of the debtors' own personal data, however, changes markedly when the debtors experience negative financial or business consequences of the processing of their personal data, especially their being registered in the central credit information system, or when they happen to default of paying back the loan in time.

Processing of personal data in connection with credit scoring is rarely publicized in Hungarian media, and if publicized, mostly as stories of financial damage of the debtor, or maladministration by bank employees, and not as an independent phenomenon. Articles about the advantages of the positive debtors list reflect, understandably, the approach of the financial institutions; communiqués about its disadvantages and questionable legal grounds were issued mainly by the Parliamentary Commissioner for Data Protection and Freedom of Information, reflecting his position (until the abolishing of his office), while news and articles about complaints and court cases generally present the complainants' aspects. Longer

analyses in the latter subject often include interviews with competent experts from the financial institutions, too.

Credit scoring organizations proved to be rather resilient towards legal and administrative limitations to their data processing practices in the long run, since they managed to establish the legal grounds for extending the scope of the debtors list to “positive” debtors (despite the long-standing opposition by the Parliamentary Commissioner for Data Protection and Freedom of Information) and they also succeeded in extending the scope of the processed personal data as well as applying new data analysing tools and methods. Citizens’ resilience towards data processing practices in the area of credit scoring is limited to doctoring of the system: in smaller places of residence credit applicants may try to influence their acquaintances in local branches of financial institutions to circumvent the financial checks if the result of these checks may have an adverse impact on their chances in getting the loan. Applicants may also ask friends or acquaintances to falsely testify on the applicant's creditworthiness, or to produce false guarantees of his financial standing.

IRISS: WP3

Final Report

UCSC

Credit Scoring

Introduction

This case-study aims at analyzing the "credit scoring" practice, intended to be a highly discriminative practice for citizens, as the main purpose is to maintain a highly competitive financial strategy of the "credit market" for Banks and Credit Bureaus, intended to be the principal stakeholders involved in this practice. The parameters of analysis are the principle of "transparency" from the watchers perspective (i.e. Banks, Financial Institutes, Credit Bureaus) on the one side and the principle of "awareness" from the watched perspective (i.e. citizens/customers: natural/legal subjects) on the other.

We look at credit scoring through a multi-faceted socio-cultural approach that takes into account some peculiarities of the Italian context, i.e. the late adoption by Italian banks of this practice compared to other European countries and the analysis of "what the watchers" know of the "watched" as power dynamics and a general lack of transparency that seems to be related to this surveillance practice.

Moreover, specific emphasis is given to the exclusive Italian case of "*Redditometro 2.0*", although it is a brand new system (it was enforced in May 2013), intended to be a State (i.e. Revenue Agency) strategy to reduce/control the diffused tax evasion phenomenon, but at

the end it has been revealed to be a highly controversial system which can infringe upon citizens' fundamental rights (i.e. freedom, private property, privacy, etc.). In fact, it has created a sort of "Big Brother" effect, spying on the citizens' incomes/expenses, bank accounts, investments and so forth. This practice, also, has fostered forms of resilience as citizens have demanded assess to the fairness, legitimacy and *a priori*, the feasibility of such a system. Finally, it is important to underline that, although this system is already in place, the DPA introduced a provision (21 November 2013)[582] aimed at limiting the Revenue Agency's power to investigate the individuals' private life, as well as to gather their personal and sensitive data, in compliance with the basic citizens' rights (i.e. privacy, personal data respect, proportionality and accountability in respect to the information-sharing, etc.).

As far as the methodological approach is concerned, this research intends to develop a description first, and then an analysis of the Credit Scoring within the Italian financial system, on the basis of qualitative information, gathered through several secondary sources: i.e. mass-media journalistic articles, online specialized websites, judicial and extra-judicial cases[583]. An added value to this study is the information and material gathered through "privileged witnesses", i.e. experts' interviews, operating in the financial system: i.e. Private Bankers and Asset Protection Advisors, who deal directly with clients; experts of the rating models' development in Italy; representatives of Credit Bureaus (in particular CRIF S.p.A.) and journalists of *Il Sole 24 Ore* (the main national financial newspaper).

From an ethical perspective, this study gathered data from diversified sources through different approaches. The experts (i.e. financial operators and journalists specializing in financial issues) have been contacted through the official channel of UCSC (e-mails, phone

[582] DPA Provision 21 November 2013, *Redditometro: le garanzie dell''Autorità a seguito della verifica preliminare sul trattamento dei dati personali effettuato dall'Agenzia delle entrate – 21 novembre 2013,* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2765110

[583] In particular, "extra-judicial cases" refer to the cases solved by Fiscal Commissions (set down at the level of Provinces and Regions), Administrative Courts, through their sentences and the Data Protection Agency through its provisions

calls and in person), explaining to them the research aim and the nature of information necessary to conduct the survey on the credit scoring topic.

The case study, referring to judicial and extra-judicial cases, has been developed through the gathering of cases, described in this study in an anonymous form to protect the identity of citizens involved in cases where there was infringement of their rights.

The main weakness of this short contribution is the emphasis on the watchers' perspective. This is due to the fact that the majority of secondary sources often – if not exclusively - address the issue of credit scoring from the banks and/or credit bureaus angle ignoring the "significant other" involved in the relationship. For instance, there are studies on the organization of lending and the use of credit scoring in Italian banks (Banca d'Italia 2010) but literature on the impact of this surveillance technique on citizens is non-existent. While this is true as far as credit scoring is concerned, this is not always the case when looking at the income meter (*redditometro*) that has been perceived –right from the start- as a very controversial issue, extensively covered by the media. As mentioned above, resilience seems to emerge more in relation to the income meter than in relation to credit scoring.

1. The history of the surveillance practice as used by a particular organization or public authority

As this table shows (Bofondi, Lotti 2006: 24), the adoption of Credit Scoring techniques by Italian banks started in the late '80s and was increasingly implemented due to the standardized approach to credit risk endorsed by the Basel Capital Accord (2001).

Table 1: Number of Italian banks adopting credit scoring (cumulative), by purpose and year.

	Any purpose	Consumer	Mortgage	Small business
First adoption	1989	1989	1993	1993
Year				
1993	3	3	1	1
1994	4	4	1	1
1995	5	5	1	1
1996	6	6	1	1
1997	8	8	2	2
1998	13	12	5	5
1999	28	22	19	6
2000	50	37	31	14
2001	60	45	41	21
2002	76	60	54	27
2003	77	61	58	32
% of banks	23.3	18.5	17.6	9.7

The late adoption of credit scoring by Italian banks is due to several aspects. Bonfondi and Lotti emphasize the following: a) the slow diffusion of technology b) the lack –until a few years ago- of comprehensive credit bureaus c) the reliance on qualitative/soft information when dealing with customers (2006: 6). Additionally, the large amount of small banks, especially in rural areas, has probably discouraged the use of standardized techniques in favor of, as mentioned above, informal relations with customers. Only after 1998, according to Bonfondi and Lotti, has the adoption of credit scoring significantly increased (*ibid.* 8) and in early 2000 this practice started to play a major role within large banking groups (Banca d'Italia 2010). More than historical analysis on credit scoring within the national context, thus, there are data on the diffusion of this surveillance technique by banks thanks to surveys carried out by Bank of Italy.

The diffusion is also linked to several changes which occurred in the 90s that boosted the use of credit scoring, namely a noteworthy reduction in the number of banks (from 1,138 in 1990 to 779 in 2003), the privatization of commercial banks, the creation of large banking

groups and the implementation of international legal provisions, as described in section 5. The role played by ICT is also worth considering as automatic decision-making processes transformed qualitative information on customers into quantitative and comparable data.

In 2007 the Bank of Italy submitted a questionnaire to 333 banks through its branch network. The results of the study show some interesting trends as far as the (recent) history and the diffusion of credit scoring is concerned, notwithstanding that the questionnaire focused more on the use of credit scoring techniques for business lending. The late adoption of this technique clearly emerges from the data: only 10% of the sample used credit scoring in 2000 while the situation changed completely in 2006 when more than 50% claimed to have adopted this practice (Banca d'Italia 2010:26). It is also interesting to consider what kinds of information sources are included in scoring systems, one of them being qualitative information both for medium-sized, large and mutual banks (Banca d'Italia 2010: 28). Storing techniques are widely used but "they are still rarely employed to determine interest rates and loan maturities" (*ibid*.29), moreover, when it comes to decisions of whether or not lending to SMEs, credit scoring tools are "decisive" only for 18% of sample and for a third of large banks.

When looking at the development of credit scoring within the national context, there are other features to consider which have encouraged the adoption of credit scoring. Banking reorganization - such as decentralization – and the presence of foreign banks have accelerated competitive pressure in the credit markets and consequently have fostered the need for automated decision making processes.

2. Who the key stakeholders in the surveillance practice are

The "Credit Scoring" practice is a model of evaluating a (natural/legal) subject through an algorithm formula ("rating system"), composed of a qualitative and quantitative set of variables, able to make a risk assessment of a certain natural/legal subject's "credit capability".

In fact, the aim of this model is to determine the level of risk for a bank or a financial institution implicit in a natural/legal subject's request for a loan (i.e. mortgage, credit, bank guarantee, etc.), through an *a priori* credit risk assessment.

The procedure of Credit Scoring in Italy is rather articulated, as it involves different stakeholders who deal and manage "sensitive personal data" at different stages and for different purposes.

In detail, from the "watcher" perspective it is possible to identify the following stakeholders:

-**Banks** (for this research analysis, UniCredit Bank[584] has been contacted as it is one of the biggest and most representative banks in Italy)

-**Private Institutions**: i.e. "*Credit Bureaus*" (CRIF[585] and EXPERIAN[586])

-**Public Institutions**: the Bank of Italy (*Banca d'Italia*)[587] and its related Central Credit Register (*Centrale Rischi* - CR)[588]

[584] www.unicredit.it
[585] www.crif.it
[586] www.exepirian.it
[587] www.bancaditalia.it
[588] www.bancaditalia.it/statistiche/racc_datser/intermediari/centrarisk

From the "watched" perspective it is possible to identify the following categories:

-**natural subject** (i.e. private citizens or consumers: "retail credit")

-**legal subject** (i.e. "small business; medium corporate; corporate" - according to the Italian Banks classification of different kind of companies, intended as potential credit customers).

In particular, it is worth noticing that the whole system focuses its attention on the "watcher" perspective, as the new regulations that have been implemented during the last few decades (from the '90s), hampers a comprehensible access for the "watched" (intended as natural subjects, i.e. citizens or customers), who are, therefore (dis)informed about the basic procedure of Credit Scoring, because of confusing information.

Banks usually gather information directly from their customers (i.e. citizens) who want/need to access the credit market, as banks receive a set of qualitative and quantitative information from citizens about their private lives (e.g. lifestyle, social *status*, level of education, civil *status*, job situation, etc.). At the same time, banks develop agreements with the s.c. Credit Bureaus[589] whose main aim is to gather data from the banks' customers to facilitate the match of demand/offer on the financial market. In detail, banks periodically (i.e. monthly) send the collected data and related updates from their customers to Credit Bureaus. Therefore, Credit Bureaus manage centralized databases, gathering information from several banks and cross-referencing the information of the banks' customers, with other banks which have joined this system.

The outcome of this procedure is the accessibility by banks to the Credit Bureaus' databases to gather further information about its customer (e.g. a customer who has several bank

[589] In Italy there are two "*Credit Bureaus*" active on the financial market: i.e. CRIF and EXPERIAN, although CRIF is the bigger one. Besides, it is important to note that both of them are private companies

accounts in different banks; a customer, who asked for a loan, is identified as a good-payer through his/her "bank history" as s/he is punctual in paying her/his debt to the bank; etc.).

Credit Bureaus' databases provide helpful information to banks in order to identify potential "positive" targets (i.e. potential new customers), to address their financial marketing campaigns (e.g. new financial products: namely, investments, life-insurance, loans to certain categories of subjects, etc.).

A further aim in the partnership between banks and Credit Bureaus is to prevent potential frauds perpetrated by customers against banks or to assess the level of solvent capability from a wider perspective, through a complex "customer profiling" system.

In this context, the Bank of Italy has a *super partes* role, as it aims to rule the monetary policy and control the overall procedure, involving the different (abovementioned) stakeholders. Therefore, it is important to note that this public institution has its own Central Credit Register (i.e. *Centrale Rischi* – CR)[590], which is a public database whose goal is to verify the information-sharing activity between the Banks & Credit Bureaus and between the Banks & Customer (i.e. natural or legal subject).

The concepts of "transparency" and "awareness" are interlinked, as the "transparency" of the Credit Scoring procedure from the "watchers" perspective depends on the level of "awareness" of the "rating system" from the "watched" perspective and *vice versa*. In this case study a lack of transparency as far the overall practice is concerned seems to emerge. In particular, the "watched", namely natural and legal subjects, have to deal with a complex landscape of regulations and information that can be misleading and can ultimately result in

[590] Banca d'Italia, *Centrale dei Rischi-Foglio informativo*, in Circolare della Banca d'Italia n.139/91, "Centrale dei rischi. Istruzione per gli intermediari partecipanti", http://www.bancaditalia.it/serv_pubblico/elenco-dei-servizi/info_archivi_CR/links/per-approfondire/foglio-informativo-CR.pdf

a low level of awareness. This is perhaps also due to the limited interest of the mainstream media, as shown in section 4.

3. What controversies have arisen in the history of that surveillance practice. Who was involved and how was it resolved?

The literature defines "Credit Scoring" as a "*credit risk management technique that analyses the borrower's risk*". This system has a discriminative *ratio*, as "*a good credit scoring model has to be highly discriminative: high scores reflect almost no risk and low scores correspond to very high risk*", the justification of this system is based on the assumption according to which "*the more highly discriminative the scoring system, the better are the customers ranked from high to low risk*"[591]. This premise reveals that the Credit Scoring system has been always perceived and improved from the Banks and Financial Institutions perspectives and interests, while the customers have advantages from this model only when they have a high rating (= low risk) as their access to loan requests is facilitated by the system itself.

Therefore, controversial issues are implicit in the Credit Scoring system and they cover a wide *spectrum* of interests of different nature:

- the information procedure and campaign from both qualitative and quantitative perspectives to the consumer on the Credit Scoring practice, involving different stakeholders (Banks, Financial Institutes, Credit Bureaus, the Bank of Italy, mass media, Consumer Associations, etc.) (watchers perspective: transparency concept)

[591] Van Gestel T., Baesens B., *Credit risk management – Basic concepts*, Oxford University Press, 2009, p. 93, http://www.wafaa-sherif.com/new/ar/wp-content/uploads/2012/11/Credit%20Risk%20Management%20-%20Basic%20Concepts.pdf

- the knowledge of the citizen of his/her rights concerning the sensitive data gathered and managed for the "rating system", as well as new financial regulations which contribute in creating a diffused misunderstanding of the Credit Scoring procedure from the consumer's perception (watched perspective: awareness concept)
- the consumers' risks referring to the personal data related to the Credit Scoring practice in light of the complex legislative framework, which contributes in confusing the private individual when making a distinction between the perceived risks and the concrete ones ("Big Brother" effect)

As far as the main issue of controversies is concerned, the data-access right is the most diffused, as it is a wide concept that covers many aspects related to the abovementioned issues: i.e. from the information right referring to personal data, to the modality of data management, procedure and timing in accessing this right.

There are two different ways to solve controversies: the judicial context (i.e. courts) and the extra-judicial context (i.e. legal demand to the DPA). It is important to note that these two approaches are mutually exclusive.

An example of a controversy solved at the level of judicial authority is the case of a citizen who obtained a loan granted by a financial institute (Compass S.p.A.) and, because of his insolvency, he had a negative rating in the Credit Bureau (Experian Information Service S.p.A.) database. This subject was financially stigmatized as any banks would have denied him, for instance, any further loan request.

This customer submitted a data access request to Compass S.p.A., as he wanted to know the details of his "credit profile", but he never received an answer[592]. In light of this, the

[592] This citizen made an appeal on the basis of art. 7 of the DP Code (d.lgs. n.196/2003), i.e. personal data access rights

citizen brought Compass S.p.A. to court claiming his data access right. The case arrived at the Supreme Civil Court (i.e. *Corte di Cassazione Civile*), which sentence underlined that, despite art. 8 DP Code not containing a precise term, the data controller is obliged to answer the data access request[593], the timing in answering a data access request can be inferred through a combined interpretation of arts. 145 and 146 of the DP Code, focused on the procedural aspects of claims. In fact, the procedure defined by the DP Code, determines a term of 15 days within which the data controller is obliged to answer the citizen's request[594].

An example of an extra-judicial controversy is the case of a citizen who appealed to the DPA (14 May 2013), as she wanted to remove, via Credit Bureau CRIF S.p.A., two real estate liens recorded in the Public Registers on 16 September 1997 and 23 March 1998 respectively, which hampered her access in obtaining credit from banks. In fact, her lawyer confirmed that the judge of the execution proceeding had already ordered the cancellation. The woman asked CRIF S.p.A. to remove these data because of the long time that had elapsed from the liens' initial registrations and because, in the meanwhile, she had repaid the debt.

CRIF replied that the data referred to liens that are stored in databases managed exclusively by the "Tribunals Information and Real Estate Registers" and CRIF simply accesses these databases to facilitate banks in gathering further information[595].

---

[593] Art. 8, comma 1, DP Code, "Exercising the rights": *The rights expressed in art. 7 are exercised through an informal request addressed to the data controller or data processor, even through a delegated subject, to whom the data controller/processor has to answer without delay*.
[594] Cassazione Civile, Sez. I, 9 January 2013, Sent. n. 349, www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Norme%20e%20Tributi/2013/01/corte-cassazione-sentanza-349-2013.pdf ; Pignatelli M. L., *La tutela della dignità e della riservatezza nel trattamento dei dati personali (Cassazione civile, sezione I, sentenza 09.01.2013, n. 349)*, 17 March 2013, www.dirittifondamentali.it/unicas_df/attachments/article/99/cass.%20civ.%20349.13.pdf
[595] DPA Provision, 19 September 2013, n. 414, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2725127

Both these (judicial and extra-judicial) cases are representative of the fact that citizens are often victims of their rights' infringement because of unclear and articulated procedures, which require an official intervention and interpretation by (extra-)judicial authorities to protect citizens' rights and interests.

Furthermore, the fiscal issue, i.e. the "*Redditometro* 2.0" system, has been the object of controversial opinions and debates at various levels, from the judicial level[596] to the mass media channels of communication[597], involving different sensitive related issues, as follows:

- the potential infringement of the "bank confidentiality" principle
- the potential infringement of the citizens' "privacy" right and the related Constitutional principles (among which are the freedom principle, the private property right, etc.)
- the lack of "transparency" in its application (the only clear information from the Revenue Agency -*Agenzia delle Entrate*- has been that the *Redditometro* system has a retroactive effect, as the fiscal monitoring of the citizens begins from the year 2009)
- the defense procedure, once a citizen is invited to give detailed explanations about some expenses or incomes sources belonging to his/her patrimony (for instance, financial investments, investments in the real estate market and, even, a simple purchase of a new car, under certain conditions)

In fact, from the moment the *Redditometro* was enforced, 35.000 letters of inspection have been sent to citizens although the DPA has not expressed its consent yet, in relation to the

[596] Commissione Tributaria Provinciale di Reggio Emilia, Sez. 2, 18 April 2013, Sent. n. 74.02.13; Tribunale di Napoli - Sez. Civile distaccata di Pozzuoli, Proc. n. 205/2013, 21 February 2013, Pozzuoli_redditometro-ordinanza-giudice—redditometro.pdf

[597] Padula S., *Redditometro, niente accanimenti*, in Il Sole 24 Ore, 4 June 2013, www.ilsole24ore.com/art/commenti-e-idee/2013-06-04/redditometro-niente-accnimenti-072238.shtml?uuid=ab6zWv1H; Trovati G., Santacroce B., *Pronte le liste per gli 007 fiscali. partono i test sul redditometro*, in Il Sole 24 Ore, 4 June 2013, pp. 1, 3; Barone N., *"Lotta all'evasione ondivaga"*, in Il Sole 24 Ore, 4 June 2013, p. 2

potential infringement of privacy right. The result has been an immediate reaction of citizens, who brought the Revenue Agency to both fiscal commissions[598] and judicial[599] courts.

The majority of the sentences on this issue are in favor of citizens' rights. For example an ordinary magistrate (Tribunal of Naples) claimed that the *Redditometro* system is "*operating outside the constitutional and European legitimacy*", as the Revenue Agency does not have "*the power to gather all the personal and sensitive data of an individual and his/her family*". Besides, the judge drew attention to the infringement of arts. 2 and 3 of the Italian Constitution and to the Charter of Fundamental Rights of the European Union. Therefore, according to the Judge of the Naples Tribunal this fiscal control system "*is not only illegitimate, but radically null and void"*, because it *"infringes upon the legal principles of equality, reasonableness, proportionality*"[600].

Therefore, it seems that the *Redditometro* has been assessed, both by citizens and judicial authorities, as a tool which might infringe fundamental rights. The system has been perceived as highly invasive and has generated what we might call "resilient attitudes" from citizens and judges alike. Resilience has emerged more in relation to this tool than to the practice of credit scoring for reasons that are difficult to grasp and go beyond the aim of the case study. However, one might speculate that the *Redditometro* was described in detail in the media and was hence more "transparent" in comparison to credit scoring.

4. How, where and when it has been referred to in the media

[598] Commissione Tributaria Provinciale di Reggio Emilia, Sez. 2, 18 April 2013, Sent. n. 74.02.13
[599] Tribunale di Napoli - Sez. Civile distaccata di Pozzuoli, Proc. n. 205/2013, 21 February 2013, Pozzuoli_redditometro-ordinanza-giudice—redditometro.pdf
[600] Greco A. M., *I giudici arrestano le tasse «Il redditometro è nullo»*, in Il Giornale, 27 September 2013 , p. 10

The most important national mass media in general, as well as the specialized newspapers (*Il Sole 24 Ore*[601], *Norme & Tributi*[602], *Plus24*[603], etc.) in Italy have a limited interest in the Credit Scoring issue, as their attention through the years (from the '90s, when the practice of Credit Scoring was introduced in the Italian financial system) has always been devoted to the "rating system" applied to Companies and Corporates (legal subjects), rather than private citizens/consumers (natural subjects).

The only two focuses referring to private individuals are mortgages and the brand new tax compliance system (the s.c. "*Redditometro 2.0*").

The mortgage issue has become particularly relevant throughout the last few years (from 2008 up to the present time), in light of the international economic crisis, as the bank system changed the parameters for customers asking for a loan ("rating system"). The natural consequence has been an overall reduction in the number of mortgages requests to the bank as the mortgage costs progressively increased[604]. Besides, the rate of those whose mortgage request has been accepted by the banks, has been progressively decreasing: only 7% of the mortgage applications are successfully satisfied by banks in the North of Italy, while in the South the percentage decreases to under 5%.

Furthermore, it is possible to analyze the differences between the North and the South of Italy in terms of the average age of citizens who ask for a loan, as well as the length, in terms of time, to repay the bank: in the South the average age for customers asking for a loan is 40 years old, compared to 37 at a national level; besides the loans have an average duration of 24 years, compared to average 22 years at a national level. On the contrary,

[601] www.ilsole24ore.com
[602] www.normeetributi.it
[603] www.ilsole24ore.com/finanza-e-mercati/plus24.shtml
[604] Cellino M., *Lo spread BTp-Bund è sceso, ma mutui e prestiti restano troppo cari*, in Il Sole 24 Ore, 6 June 2013, www.ilsole24ore.com/art/notizie/2013-06-06/spread-btpbund-sceso-mutui-105921.shtml?uuid=AbgpLd2H&fromSearch

there are no particular differences in selecting the typology of interest rate: the fixed rate of interest is always preferable[605].

Therefore, a further consequence of this situation is the freezing of the real estate market (indirect consequence)[606], since the majority of the mortgage applications by the citizens are for buying a residential home (house/apartment). In fact, the Italian situation reveals that the citizens have many economical disadvantages, due to the weak Italian institutional and political conditions, which negatively influence the financial market, compared to the international/European situation in other countries.

In particular the "spread" in the case of mortgages, for buying real estate property, is still high (an average cost of 3%), and it is even higher, considering the Irs and Euriobor Indexes.

Banks often justify this situation, not only with pure financial and political reasons, but also in light of a progressive risk increase in granting loans to Italian citizens, because of economic recession phase that has been in place for a long time, as well as the recent adoption of more restrictive measures from an economic perspective (i.e. reduction of public and private costs, increase of tax rates, etc.), but, as a result, Italian families pay a higher cost for credit access compared to the European standard[607].

[605] Il sole 24 Ore, *Mutui, ok solo al 7% delle richieste. E al sud si scende sotto il 5%*, in Il Sole 24 Ore, 8 June 2013, www.ilsole24ore.com/art/finanza-e-mercati/2013-06-18/mutui-solo-richieste-scende-102105.shtml?uuid=AbqxIz5H&fromSearch

[606] Sgambato E., *Crollo dei mutui e prezzi ancora alti bloccano il mercato immobiliare*, in Video.ilsole24ore.com/Casa24/Video/mercato-immobiliare/2013/mercato-immobiliare-compravendite-sgambato/meracto-immobiliare-comprevendite-sgambato.php

[607] Cellino M., *Lo spread BTp-Bund è sceso, ma mutui e prestiti restano troppo cari*, in Il Sole 24 Ore, 6 June 2013, www.ilsole24ore.com/art/notizie/2013-06-06/spread-btpbund-sceso-mutui-105921.shtml?uuid=AbgpLd2H&fromSearch

The "*Redditometro 2.0*" system, instead, has been recently reformed, as it has been enhanced in May 2013 with the "Tax Register Information System" ("*Anagrafe Tributaria*")[608], a complimentary tool, managed by the banks (through their customers databases) in collaboration with the "Revenue Agency" (*Agenzia delle Entrate*)[609]. This system implicitly involves different stakeholders: i.e. the Revenue Agency, Banks and Financial Institutes and the citizens (natural/legal subjects). The diffused perception of this instrument has been the creation of a "Big Brother" effect, where the citizens are "spied upon" by the State, able to monitor the lifestyles of its citizens, who are forced by the necessity to justify any expense/income or investment in their private life.

The mass-media in fact devoted great attention to this issue, describing it as an invasive tool into citizens' privacy, through the exploitation of the banks' databases and information gathered from their customers.

At a first, mass-media focused their attention on the new set of rules implemented by the Revenue Agency: i.e. the procedure of inspections[610], the timing of inspections (from 2009 on), the cross inspection based on the lifestyle of the citizen (i.e. personal patrimony) and the data gathered in the "Tax Register Information System", etc.[611]. The Revenue Agency has now direct access to both bank accounts and financial investments of customers[612].

A second aspect pointed out by the mass-media is the legal framework. As described in section number 3, the implementation of the *Redditometro* provoked the reaction of citizens

---

[608] Acierno R. and Parente G., *Bonus sotto la lente del redditometro*, in Il Sole 24 Ore, 9 September 2013, p. 5
[609] www1.agenziaentrate.gov.it
[610] LeggiOggi, *Nuovo Redditometro 2013:: come spiegare il discostamento del 20%*, 5 August 2013, www.leggioggi.it/2013/08/05/nuovo-redditometro-2013-come-spiegare-il-discostamento-del-20/print; Salvaggio A., *Cosa fare se arriva il questionario del redditometro*, 16 September 2013, in Fisco7
[611] Deotto D., *Il nuovo redditometro vale dal 2009*, in Il Sole 24 Ore, 1 August 2013, p. 3; Trovati G., *Più selezione prima della verifica*, in Il Sole 24 Ore, 1 August 2013, p. 3; Cipriani N., *Arriva la circolare: decolla il nuovo redditometro*, 1 August 2013, in Fisco7; Il Quotidiano del Fisco, *Nuovo redditometro: verifica sulle spese*, 18 September 2013, www.quotidianofisco.ilsole24ore.com/art/oggi/2013-09-18/nuovo-redditometro-verifica-spesa.php?print=si
[612] Bellinazzo M., *Pronte le lettere per il redditometro*, in Il Sole 24 Ore, 5 September 2013, p. 5; Cipriani N., *Redditometro: i risparmi giustificano gli incrementi patrimoniali*, 28 August 2013, in Fisco7

challenging [613] the system from different perspectives: namely, the intrinsic validity of the statement of assets and liabilities parameter for the investigation[614], which has been discussed by the Province/Regional Fiscal Commissions, right up to appeals to the Supreme Court (i.e. *Corte di Cassazione*)[615]; the potential infringement of personal data and citizens' privacy, through a direct access of the *Redditometro* instrument to several databases of private and public institutions, (*primus inter pares*, the bank and financial institutes' databases)[616].

Furthermore, on the Internet, there are several resources (from websites[617] to more informal blogs[618]) which convey relevant information and even simulate loan requests. From this perspective, the Internet plays a key role in increasing the level of awareness concerning credit scoring.

5. When, where and how it has been implemented; who led the implementation. Who else was involved in it?

[613] i.e. *Commissione Tributaria*
[614] Commissione Tributaria Provinciale di Campobasso, sent. n. 117/2013 and Commissione Tributaria Provinciale di Bari, Sent. n. 146/2013; Commissione Tributaria Regionale della Campania, Sent. n. 25481/2008, in Alberici D., *Nuovo colpo al redditometro*, in Il sole 24 Ore – Imposte e Tasse, 26 September 2013, p. 8
[615] Corte di Cassazione, Sez. Tributaria, 25 September 2013, Sent. n. 21994, in Fisco e Diritto, 25 September 2013, www.fiscoediritto.it/corte-di-cassazione-sezione-tributaria-sentenza-25-settembre-2013-n-21994/
[616] Greco A. M., *I giudici arrestano le tasse "Il redditometro è nullo"*, in il Giornale, 27 September 2013, p. 10
[617] http://www.economianews24.com/che-cosa-e-il-credit-scoring-guida-al-credit-scoring-377.html; http://guidaaiprestiti.blogspot.it/2010/09/cosa-e-il-credit-scoring.html

[618] http://assicurazioniebanche.blogspot.it/2009/06/mutui-che-cose-il-credit-score.html; https://promotoremutui.wordpress.com/tag/credit-scoring/; http://www.prestiti.it/credito-consumi/credit-scoring-e-rischio-di-credito; www.isolamutui.it/sito/guida-ai-mutui/centrale-rischi

Credit Scoring is a quite recent practice, as it has only been introduced in the Italian financial system through the 1990s.

The implementation of this system has been determined *in prims* by the international legal provisions (i.e. the "Basel" system). Further interventions in the Credit Scoring procedure have been adopted by several stakeholders on the basis of their role within the whole procedure: the Banks adopted the "rating systems" for reducing/controlling the risks related to the "credit market", especially from the 2008 up to the present time, in light of the international economical crisis and they periodically update their "rating system" (algorithm models) according to market changes. In consequence, the Credit Bureaus keep enhancing their databases to facilitate the credit demand/offer market, as their role is to create a network of connections between the Banks/ Financial Institutions and the citizens/customers (natural/legal subjects). In fact, practically the system is based on an exchange of information between the Banks, which update their customer data monthly and transmit this to the Credit Bureaus (i.e. CRIF) databases, while the databases held by CRIF, as well as those managed by the other Credit Bureaus, are available to the Banks for a cross check aimed at making an *a priori* risk assessment, before granting a loan to a consumer.

Finally, the Consumer Associations[619] have a marginal role in the financial system, as in Italy they do not have a significant influence, although they are often used as an additional publicity/information channel to improve the knowledge level of the potential customers when accessing the credit system.

In particular, these associations do not act autonomously, but in collaboration with private and public institutions, supporting the role of these entities. An example of partnership

[619] Adiconsum: www.adiconsum.it; Assoutenti: www.assoutenti.it; Codacons: www.codacons.it; Federconsumatori: www.federconsumatori.it

between a Consumer Association and a private institution is *Altroconsumo*, that, in collaboration with CRIF, drafted a handbook[620]. Besides, an example of collaboration of these associations with public institutions is *Federconsumatori* Sicily and the Presidency of the Sicily Region, which, in 2009, drafted another handbook addressed to the citizens of the Sicily Region to inform them about the procedure to access the credit market[621].

6. How it is currently regulated

The regulation analysis of "Credit Scoring" is developed through a three-level approach:

1. **International level**
2. **European level**
3. **National level**

In detail, the "Credit Scoring" procedure is based on a set of *super partes* rules, enforced at an **international level**, the s.c. "Basel" system. Through the decades and in line with the international economic dynamics evolution, this system has been the subject of several modifications.

A brief historical *excursus* of this system is necessary to understand the framework of rules in which Credit Scoring developed, improving little by little the specificities of each national economical and financial "market" tradition and culture, among which is the Italian one.

[620] Vademecum, "*Conoscere i sistemi di informazioni creditizie (casa deve sapere il signor Rossi nel caso in cui richieda un finanziamento per acquistare l'auto piuttosto che l'abitazione)*", www.crif.it/Documents/Vademecum_Informazioni_creditizie.pdf
[621] Matteini G., *Guida al funzionamento dei sistemi di informazioni creditizie*, 2009, www.ioconsumatore.eu/wp-content/uploads/2010/09/InformazioniCreditizie.pdf

The Basel Committee was created in 1974 and was aimed at controlling the international banking system to guarantee a stable global financial model as much as possible. This committee is composed of representatives of several Central Banks of different Countries that make up the G10. The headquarters of this international organization is in Basel. This committee does not have any legislative enforcement capability, but it can propose the main rules and directives that each County should adopt and adapt within its specific legal system.

"Basel I" is the output of a first agreement in 1988 defining the minimum standard patrimony of the Bank to limit the financial speculation policy of certain banks. To achieve this goal, it was essential to regulate the "credit risk" and the "market risk". In 1999 this agreement was the subject of revision and update through the implementation of the bank control system, the s.c. "Basel II", introducing a "rating system" to enable the banks e to limit the risk of the credit market. Paradoxically, the system was aimed at strengthening the *resilience* of the banking sector (Consultative Document 2009). This agreement was enforced on 1st January 2008. During the most recent economic and financial crisis, the Basel model has been further updated, introducing "Basel III", which should be enforced by 2013 (through a transition period that will last till the 1st January 2019), aimed at preventing the increase of risk levels for the banks, to make the financial system more stable and unify the international financial rules, through the introduction of a set of rules that are generally accepted[622].

At a **European level** the EU Directive 95/46/EC "*on the protection of individuals with regards to the processing of personal data and on the free movement of such data*" [623] is at the base of any national legal provision for personal data retention, including the Italian legal framework on the Credit Scoring practice specifically referring to sensitive data gathering

[622] Orsini C., *Da Basilea 1 a Basilea 3*, Arcadia Consulting Srl, Bologna, 2010, www.arcadiafinance.eu
[623] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, in OJ L 281/31-39, 23.11.95

and management (*ad hoc* databases) by the different financial stakeholders involved in this procedure.

As a consequence, at a **national level** the legislative framework focuses its attention on the Credit Scoring procedure which is perceived as a surveillance practice. Therefore, this system has been the subject of specific intervention by the DPA, which enforced detailed rules for data collection and management of consumers. The "Data Protection Code"[624] (DP Code) has devoted an *ad hoc* part of the Code to the financial issue, focusing attention on the data retention and management in this context.

The DP Code, Part II – "*Dispositions referring to specific sectors*", Title IX – "*Bank, financial and insurance systems*", Capo I – "*Information systems*"[625] describes the set of rules addressed to data collected in the financial and insurance systems for different purposes and its protection:

Art. 117 – "*Reliability and punctuality in payments*"

Art. 118 – "*Commercial information*"

Art. 119 – "*Data referring to the debtor's position*"

Art. 120 – "*Accidents*"[626]

In addition, the DP Code was implemented in 2005 with an Enclosure (*Allegato*) A.5 entitled "*Deontological and good conduct code for the information systems managed by private*

[624] D.L.gs 30 June 2003 n. 196, in G.U. 29 July 2003 n. 174 – Supplemento Ordinario n. 123
[625] Artt. 117-120, D.L.gs 30 June 2003 n. 196, in G.U. 29 July 2003 n. 174 – Supplemento Ordinario n. 123, pp. 32-33
[626] This concept is specifically referring to the "insurance" context

subjects on the consumers' credit, customers' reliability and punctuality in payments"[627], specifically addressed to the financial stakeholders involved in the gathering and management of the citizens' personal data.

This deontological code is the result of private subjects' pressure (i.e. consumer associations and class associations)[628], aimed to protect, through the DPA intervention, consumers within the topic context of sensitive data referring to the credit market, as well as commercial activities in general. This code is addressed exclusively to private institutions (i.e. Banks, Credit Bureaus, Insurance Companies, Financial Institutes, etc.) and their related databases, excluding databases managed by public entities (i.e. Bank of Italy and Central Credit Register)[629]. This deontological code contains a set of rules aimed at defining the subjects entitled to gather, manage and store sensitive data on customers (art. 1-7); the consumers' rights to access their data (art. 8); management of Credit Scoring databases (art. 9); management of data from public sources (art. 10); security measures and devices to store sensitive data (art. 11); sanctions (art. 12); final dispositions (art. 13) and enforcement procedure (art. 14).

As far as the *Redditometro* system is concerned, the DPA implemented an *ad hoc* provision[630], regulating the access to the "Tax Register Information System" by banks and financial institutions. In fact, the Tax Register Information System is composed of sensitive data gathered from the financial entities, aimed at collecting financial information for measuring the patrimony (incomes/expenses) declared by individuals, to verify the

[627] DPA Provision 16 November 2004, n. 8, in G. U. 23 December 2004 n. 300, modified with a corrigendum (*errata corrige*) as published in the G. U. 9 March 2005 n. 56, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1556693

[628] DPA Provision 10 April 2002, in G. U. 8 May 2002, n. 106, www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1070020

[629] Preamble, point 6., DPA Provision 16 November 2004, n. 8, in G. U. 23 December 2004 n. 300, modified with a corrigendum (*errata corrige*) as published in the G. U. 9 March 2005 n. 56, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1556693

[630] DPA Provision 17 April 2012, n. 145, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1886775

compliance of that information with their tax declaration (i.e. *Redditometro*). The final aim of this system is to reduce/control tax evasion. These rules have been implemented with a further DPA provision[631].

Finally, it is important to notice that the DPA, analyzing the *Redditometro* system[632] has recently promulgated a provision[633], specifically referring to this fiscal tool. The original idea of *Redditometro*, in fact, has been modified for compliance with the citizens' fundamental rights, according to the Italian Constitution and the European Human Rights Charter (i.e. privacy and data protection rights)[634].

In particular, the DPA has defined certain rules for the application of the *Redditometro* by the Revenue Agency, to protect citizens' privacy[635]:

-the inspection is addressed only on actual expenses, as it could not refer to estimated expenses, on the presumptive base of the *Istat*[636] standards. The "concrete expenses" are proved also through specific forms of payment (i.e. bank transaction, bank cheque, credit card transaction, etc.). It is possible to pay by cash, but in this case the amount is limited to one thousand Euros. This is the s.c. "profiling principle";

---

631 DPA Provision 15 November 2012, n. 861, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2099774

632 Parente G., *Il Garante della privacy punta i fari sul redditometro*, in Il Quotidiano del Fisco, 19 September 2013, www.quotidianodelfisco.ilsole24ore.com/art/oggi/2013-09-19/garante-privacy-punta-fari.php?print=si; Celletti A., *Fisco e Privacy non sono nemici*, DPA, Interview to Antonello Soro – DPA President, in Avvenire, 9 January 2013

633 DPA Provision 21 November 2013, *Redditometro: le garanzie dell''Autorità a seguito della verifica preliminare sul trattamento dei dati personali effettuato dall'Agenzia delle entrate – 21 novembre 2013,* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2765110

634 La Repubblica, *Redditometro, via libera dal Garante. Ma detta anche le modifiche da fare*, 21 November 2013, http://www.repubblica.it/economia/2013/11/21/news/redditometro_garante_privacy_d_il_via_libera_ma_con_alcune_modifiche-71543171/?ref=HRER2-1

635Federprivacy, *Il Garante detta le regole per adeguare il redditometro alla normativa privacy*, 21 November 2013, http://www.federprivacy.it/index.php?option=com_content&view=article&id=1028&Itemid=64; La Repubblica, *Redditometro, via libera dal Garante. Ma detta anche le modifiche da fare*, 21 November 2013, http://www.repubblica.it/economia/2013/11/21/news/redditometro_garante_privacy_d_il_via_libera_ma_con_alcune_modifiche-71543171/?ref=HRER2-1; Trovato I., *Effetto privacy sul redditometro, via pentole e vestiti dal modulo*, in Corriere della Sera, 22 November 2013, p. 5

636 Istat – *Istituto Nazionale di Statistica* (i.e. National Institute of Statistics), www.istat.it

-the Revenue Agency has to factually verify the composition of an individual's family, for the inspection of the real expenses;

-the Revenue Agency should pay careful attention to the quality and accuracy of the gathered data, as the inspection needs to avoid discrepancies between the "fiscal profile of an individual" and the "civil status" of this person;

-the taxpayer has the right to be properly informed that his/her personal data are subject to investigation, according to the *Redditometro* system (for instance, a specific clause in the tax declaration application has to be introduced to inform taxpayers on their personal data use and gathering);

-the *Redditomerto* system has to guarantee the "cross-examination principle", as the citizen has the right to prove the legitimacy of his/her expenses, in relation to his/her income (i.e. personal lifestyle). Besides, any taxpayer has the right to be informed about the consequences (e.g. sanctions) of refusing to provide the Revenue Agency with the documents to prove his/her legitimate expenses.

7. Whether the practice is externally accountable, and if so, to whom

The Credit Scoring issue is based on an extremely technical procedure, which is strictly regulated at different stages (both at super-national and national levels), therefore it is possible to define this practice as a "self-referential system".

The responsibility and the explanation of the system is basically managed by the internal Credit Scoring stakeholders directly involved in this practice.

The external interference and accountability for the system is circumscribed in certain aspects of the whole procedure. It is the case, for instance, for the natural subject to gain data access through the Consumer Associations filter, although it is possible only for Credit Bureau (e.g. CRIF) database access and the procedure is strictly regulated with *ad hoc* dispositions, as most consumers prefer to contact the CRIF or EXPERIAN personally, firstly to shorten the whole procedure and because of the lack of information about this service (i.e. CRIF website). Finally, it is also important to note that the rate of access requests through these kind of associations is extremely low, almost marginal for the statistical data gathered by CRIF.

8. How the organization or public authority has engaged with the public around its use of the surveillance practice

The watcher perspective analysis of the connection between the financial stakeholders and the citizens/customers is a multi-level approach.

The interaction of the Financial Institutions with the public differs according to the topic stakeholder involved in the Credit Scoring procedure and the different exchange of information on this surveillance practice can be summed up as follow:

- ***Bank – Citizen***

The contact between the Bank and the customer/citizen is frequently established through a Private Banking Consultant, i.e. a direct relationship between these two subjects for the advantage of both the parties involved in the credit procedure.

In fact, the Bank needs, to a certain extent, the personal contact with a (potential) customer, as it represents one of the privileged channels of surveying to collect (qualitative and quantitative) information about the client's life, profession, activity and patrimony, which can help the Financial Institutions to make an effective risk assessment in case of a loan request.

On the other hand, the citizen has a direct channel of information from the Bank, to whom to address his/her technical explanation requests, as well as freely explain the necessities in his/her everyday life.

Therefore, the "rating models" developed by the Banks for the credit market are implemented and updated on the basis of the information exchanged and collected from the direct interaction between the Bank and the client.

- ***Bank – Credit Bureaus***

The relationship between these two financial stakeholders is the result of a mutual exchange of information and experience.

Each Bank is free to stipulate a contract with Credit Bureaus, in Italy the major one is CRIF, on the basis of which the Bank transfers all the information about its clients, updating them monthly, to the CRIF database system (SIC = system of credit information), called EURISC. The Bank's advantage is an open source access to the CRIF database to collect further information about its customers (e.g. a client who may have several bank accounts with different Banks) for making research, as well as for a more effective risk assessment and attributing a more realistic "rating" to its client.

A further advantage in collecting information from the CRIF database is the capability in developing more effective marketing strategies, as the financial products offered by the Banks better mirror the public expectations.

On the other hand, CRIF has the opportunity in gathering a wide *spectrum* of information from the Financial Institutions, so that it can produce statistical data about the financial and credit market trends, as well as developing "rating systems", through the implementation of a consultant activity by the "CRIF Credit Rating Agency" addressed to the Financial Institutions[637].

- ***Credit Bureaus - Citizen***

The interest of the Credit Bureaus in developing contacts directly with the public at large are limited, as the information is gathered from the Banks and the Financial Institutions.

The CRIF in particular has developed an information policy campaign oriented in improving the level of customers' awareness on financial issues, aimed at reducing financial fraud, as well as offering some services to consumers, such as the "*Mettinconto*" service[638], aimed at accessing the customer's personal financial data to create a "profile" of his/her own creditworthiness before requesting a loan from the Bank (credit simulation system). It is also useful for planning the financial future of a customer, through a better knowledge of the possibilities and limits of his/her financial "profile".

9. How members of the public have engaged with their data doubles and the organizations who use the surveillance practice

[637] www.creditrating.crif.com/Pages/default.aspx
[638] www.crif.it/Consumatori/Mettinconto-scopri-il-tuo-merito-creditizio/Pages//Che-cos-è-METTINCONTO.aspx

The watched perspective analysis of the Credit Scoring surveillance practice of the citizens by the Financial Institutions and authorities is more limited, as there are few channels of communication and information collection for the public at large.

Therefore, the different perspectives of observation from the customers' point of view are the following:

- ***Citizen – Bank***

The customer's opportunity to collect technical information and request detailed explanations or clarifications is based on his/her interaction with a Private Banker Consultant.

In fact, whether the citizen needs to apply for a loan or in case of a denied loan, asking for the reasons for the denial, the Private Banker Consultant can give the client an answer about his/her rights and financial "profile". In particular, the client of the Bank can also request information about his/her personal "rating", calculated by the Bank (through an algorithm model) and the Bank is obliged to answer this question, although it will never give a detailed explanation on the model at the base of the "rating system" developed by the Bank itself.

- ***Citizen – Credit Bureaus***

The Credit Bureaus and, in particular CRIF, have implemented several channels through which they may be contacted directly by the citizens/customers, although CRIF has no direct relation with the private individuals, having only contracts specifically stipulated between the Banks/Financial Institutions and CRIF itself. Therefore, contact with the citizen is necessary whether there is an objective need in communicating modifications, updates or complaints on the personal data gathered by the CRIF database system.

The channels to contact CRIF by a private individual are the following[639]:

-Call centre

-Online procedure through the CRIF website[640]

[639] CRIF website information source: www.crif.it

-Mail system

-Fax system

-Public Relations Office (CRIF has only one head office in Bologna, which covers all of Italy)

A further channel of contact between the citizen and the Credit Bureaus, namely CRIF, are through the Consumer Associations, although these associations have a limited capability in informing the citizens about the Credit Scoring surveillance practice in general, as they can only be contacted in a specific case of personal data access right by the customer in order to access the CRIF databases[641].

Finally, it is crucial to note that the relationship between the customer and the Bank is based much more on trust and confidence, rather than the "awareness principle" of the citizen on his/her rights as client, because of several factors, among which an overruling in the financial issue are the new financial regulations; the lack of information from a quantitative perspective, as the sources are circumscribed (Bank, CRIF and very little role played by the Consumer Associations); the lack of information from a qualitative perspective, as the financial world often implicitly requires a technical background and a certain level of knowledge that belongs only to a few people, i.e. those who have the opportunity or the interest to carefully collect information on financial issues and *de relato* on the Credit Scoring practice.

10. How subject-access requests feature, and what the rates of use are

The citizens can access their own data at three different levels during the whole Credit Scoring procedure, according to which stakeholders the request refers to, although the

[640] www.crif.it/Consumatori/Pages/Consumatori.aspx
[641] www.crif.it/Consumatori/E-utile-sapere/Pages/Accordi-con-le-Associazioni-dei-Consumatori.aspx

access through Consumer Associations is not statistically representative and almost non-existent:

- personal data access requested directly from the Bank and/or Financial Institution
- personal data access requested from Private Institutions, i.e. “Credit Bureaus” (CRIF and EXPERIAN)
- personal data access requested from the Consumer Associations for accessing the “Credit Bureaus” (CRIF in particular) databases

Each stakeholder has its own procedure in accessing data dpending on the natural subject that the data belongs to and the procedures are substantially based on the DPA dispositions, referred to in the legal and provisional sources, i.e. the DP Code and the Enclosure A.5 of the DP Code (see section 6.).

The Public Institution stakeholder, i.e. the Bank of Italy, involved in the procedure, has its own database with sensitive data, but, as it is a *super partes* organ, it aims to evaluate that the procedure of Credit Scoring and the related “rating system” is in compliance with the rules and provisions laid down by law. Besides, the Bank of Italy manages a Central Credit Register (*Centrale Rischi* - CR), which links the Banks and Financial Institutions to the consumers/citizens.

A common procedure to access data consists of a consumer contacting, in the first instance, her/his bank, specifying the motivation. This request can be formulated by a written letter or orally directly to the bank employee (usually the Private Banker, who manages the relationship between the bank and the client). If the request aim is an ordinary one (i.e.

modification of civil *status*, change of home address or job situation, etc.) the bank answers the customer's request directly.

On the contrary, when the client submits a data subject request, the bank contacts CRIF directly or suggests the customer contact Credit Bureaus (see section 9) to collect more detailed information. In this second case, the customer can follow the procedures explained on the CRIF website to fill in the application form and access her/his personal data. In any case, in both hypotheses (i.e. the bank contacts CRIF or the customer contacts CRIF) the customer receives only basic information about her/his "rating" on the "credit market" scale, as financial institutions will never specify the reasons and details at the base of the "rating" attribution to the customer's profile. This is due to the fact that, behind the "rating scale", there is the application of an algorithm based on quantitative and qualitative[642] information gathered from customers. In fact, each bank or financial institute develops and periodically updates (conforming to the changes in the credit market) this formula.

Therefore, the final result is a complex procedure of "rating", which remains unclear and non-transparent for the citizen, implemented on the idea of facing the risks, among banks, of the financial market, rather than to develop a system which can be accessible and comprehensible to the public at large.

Consequently, from the citizen's perspective the outcome will be a reduced level of awareness, because of the whole credit market system, which *de relato* excludes those categories of subjects who are not able first to find, and then to understand, highly technical information, as well as specific financial market regulations.

References

[642] In the whole "credit scoring" procedure, the "qualitative information" influences a maximum of 10%, as it can vary from bank to bank according to the internal credit policy

Banca d'Italia, *Centrale dei Rischi-Foglio informativo*, in Circolare della Banca d'Italia n.139/91, "Centrale dei rischi. Istruzione per gli intermediari partecipanti", http://www.bancaditalia.it/serv_pubblico/elenco-dei-servizi/info_archivi_CR/links/per-approfondire/foglio-informativo-CR.pdf

Banca d'Italia 2010, *Banks, Local Credit Markets and Credit Supply, http://www.bancaditalia.it/pubblicazioni/seminari_convegni/banche-mercati-territoriali/5_banche-mercati-territoriali-2010.pdf*

Bonfondi M., Lotti L., 2006, *Innovation in the Retail Banking Industry: the Diffusion of Credit Scoring,* https://mail.sssup.it/~lotti/Bofondi_Lotti.pdf

Van Gestel T., Baesens B., 2009, *Credit risk management – Basic concepts*, Oxford University Press p. 93,

http://ww.wafaa-sherif.com/new/ar/wp-content/uploads/2012/11/Credit%20Risk%20Management%20-%20Basic%20Concepts.pdf

WP3 IRISS – Report on Credit Scoring in Norway: practices and controversies

Stine Bergersen, Rocco Bellanova, and J. Peter Burgess, PRIO[643]

1 Introduction

This report aims to provide an overview of credit scoring as a surveillance practice in Norway. In this country, credit scoring is a service provided by a limited number of licensed companies. Whenever a transaction implies an element of credit, the provider of the credit may require a licensed company to check the prospective beneficiaries of the credit and provide an assessment of their foreseeable ability to pay (back). From this perspective, credit scoring can be studied as a form of surveillance: according to the now seminal definition proposed by Lyon, surveillance is "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" [644].

Relying on the common outline of data gathering and analysis developed in the framework of Work-Package 3 of the IRISS project, we focus on the main practices and controversies surrounding credit scoring. The case study of Norway permits to highlight three salient aspects of credit scoring as surveillance practice. First, the relation between data protection and credit scoring is not merely a matter of limitation and protection but rather of co-constitution. The two are entangled to the point that it is impossible to analyze the one without taking into account the other. Second, while there is a substantial lack of radical opposition to credit scoring, controversy is not totally absent but somehow atomized and mostly channelled in data protection related instances. Third, credit scoring is a form of

[643] A special thank to Marit Moe-Pryce and Maral Mirshahi (PRIO) for providing *ad hoc* translations of key passages of webpages and documents, and for the preliminary exploration of media coverage of credit scoring practices and controversies in Norway. The authors would also like to thank Ann Sætan Rudinow for her precious advice and help in relation to the credit scoring cases handled by the Norwegian Privacy Appeals Board (cf. section 3.2 below).

[644] Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, p. 2.

pervasive on-demand surveillance. It relies on data from the vast majority of the population, it can be used to grant access to mundane services, and it is, de facto, at disposal of many diverse actors.

The methodology adopted consists mainly in the identification and analysis of publicly available documents and controversies. In terms of sources, the most important have proven to be national regulations, administrative judgments, annual reports of the Data Protection Authority (DPA) and websites of major credit scoring companies and popular media (mostly newspapers). In the preliminary stages of the research, exploratory off-the-record contacts with officials from the *Datatilsynet* – the Norwegian DPA – have provided a useful insight on a topic that largely remains overlooked by scientific literature.

The rest of the report is divided in three main parts. In section 2, we present and analyze the main practices of credit scoring. This includes a brief overview of the history of credit scoring, and its influence on the drafting of the first data protection legislation (2.1); a review of the main legal provisions and of the so-called licence system (2.2); and the analytical description of the current practices of credit scoring agencies (2.3). In section 3, we shift the focus on the main controversies at stake. There, we take into account the media coverage of debates surrounding credit scoring (3.1); the cases brought before the *Personvernnemnda* – the Norwegian Privacy Appeals Board (3.2); and the tensions among relevant stakeholders (3.3). Finally, in section 4 we summarize the main findings of the study.

2 Practices

2.1 History: a progressive entanglement of credit scoring and data protection legislation

The evolution of credit information services dates back to the mid-19th century. Then, the service was carried out alongside debt collecting within bank's organizational frames. Prior to the establishment of credit scoring agencies, the person seeking credit had to contact banks, suppliers etc. and gather the references needed. Eventually, the trade assumed such

forms that a central register was needed, and following, the need for credit scoring agencies. In Norway, credit information services assumed organized forms from the last decades of the 19th century, and with the evolving internationalization of trade, their activities were extended outside the country, establishing also international branches[645]. Initially, the credit information service itself required no special qualifications, and there were no particular rules regulating the service[646].

In the 1970s, concerns about the possible dangers of abuse entailing the deployment of the electronic processing of personal data were raised[647]. Among the most dreaded forms of abuse was the possibility to cross-connect different registers[648]. The increasing concern with the potential consequences of the electronic processing of personal data was the starting point for the first initiative for the implementation of data protection legislation in 1970. Two committees were appointed by the Parliament, and it is important to note that one of them was named *Kredittopplysningsutvalget* – the Credit Information Committee – because of its strong focus on credit information agencies. This committee was led by a professor of law, Tore Sandvik, and had seven additional members. Four of these were representatives suggested by credit information agencies and credit scoring agencies[649]. There was wide political consensus about the need for data protection legislation, and the debated issues at

---

[645] NOU 1974:22 *Persondata og personvern*: p. 24- 25. Both the government or a ministry can appoint committees and working groups to investigate various matters in society. Their findings are either labelled as NOU – Norwegian official reports – or as reports.

[646] *Ibid*.

[647] The deployment of data registers in public sector was the starting point of the modern privacy debate in Norway. During the 1950's and 1960's, several cases both in courtrooms and in public debate revolved around the "individuals right to be left alone", and the implementation of a national birth number system was also of influence. It could be noted that the largest Norwegian credit information agency in 1974 stated that they had no plans of replacing the traditional methods with the use of electronic data processing (NOU 1974:10:12).

[648] An example was the collaboration between the police and the bank *Kredittkassen* in 1974, where Kredittkassen hired two retired police officers to investigate costumers applying for a checking account . The bank wanted to prevent credit fraud, and, as a preventive action, the two retired police officers were given access to the police registers to make sure that convicted criminals weren't given a checking account. The applicants were not informed of this cross-checking in advance, and were not given any explanation in case of denial. This kind of collaboration was not actually illegal, but following extensive media coverage, the Minister of Legal Affairs stated that the police's criminal registers were not to be used by anyone other than the police itself.

[649] Sandvik in Blekeli and Selmer (ed.) 1977: *Data og personvern*. p. 44.

stake revolved around how to define the limits for the use of the data. The mandate of the committee was to investigate the use of personal data in private sector. The following year, the second committee, the *Datautvalget* – Data Committee – was formed to carry on the same task for the public sector. The reports of the committees, including suggestions for new legislation, were released in 1974. The Credit Information Committee proposed general rules for the registration of information in registers, and drafted the guidelines for the licence system. The Data Committee built on this work, and added suggestions about guidelines for a common regulatory authority to be responsible for the license system, and to make sure that the legal provisions were followed[650]. These two suggestions were later translated into a unified act by the Ministry of Justice, and were presented to the government as *Ot prp nr 2* (1977-78) *Om lov om personregistre m.m.* The *Personregisterloven* was adopted on the 9th of June 1978, and implemented 1st of January 1980[651]. Both the right to access her own data (Section §7) and the right to make corrections to her data (Section §8) were included in this act. Section §40 protected the individual against possible economic damage caused by use of incorrect information by credit information agencies, obliging them to replace eventual economic loss of the individual.

This brief historical overview permits to highlight how, with the introduction of the electronic processing of data and the creation of larger registers, the practices of credit scoring and data protection started getting entangled. Even if the adoption of data protection legislation is considered a form of reaction to the new surveillance technologies, the relation between the two practices is, from the very beginning, of mutual definition and construction. For example, the composition of the committee, as well as the mandate, reflected clearly the importance of credit information services. This focus made its mark in the work leading to the finalized act, with several suggestions translated into the adopted act. Among them, credit scoring was treated as a sort of *sui generis* field, where even one of the key notions of data protection, the notion of "person" – data subject in the jargon of the European Union data

[650] NOU 1974:22: *Persondata og Personvern*, p. 6.

[651] Djønne, Eirik (ed.) 1990: *Datatilsynet. Ti år som personvernets vokter*. p. 11.

protection law – had a specifically widened scope, so to include both physical and legal persons.

2.2 Legal framework: the main provisions and the licence system

Since the first Norwegian data protection legislation in 1978, data protection itself became, and still is, the main legal basis for carrying on credit scoring in Norway. Nowadays, credit scoring is legally governed by Chapter 4 of the Personal Data Regulations of December 2000 (PDR), and in particular Sections 4-1 to 4-7[652]. Chapter 4 PDR also retains the same peculiarity of the previous legislation, granting protection not only to "natural persons" but also to "other[s] than natural persons" (i.e. private firms). This widening of the scope is not limited to the guarantees listed in Chapter 4 PDR, but also grants the application of the provisions of the PDA to the latter category when it comes to credit scoring (Section 4-1 PDR)[653].

Section 4-2 PDR provides a positive definition of the term "credit information service" as "activities which consist in providing information that throws light on creditworthiness or financial solvency" (1st para Section 4-2 PDR). The same section offers also a sort of negative definition by both indentifying specific exceptions, and by making explicit all the services that "are not regarded" as such (2nd part 1st para, and 2nd para Section 4-2 PDR).

Section 4-3 PDR establishes rules for the "disclosure of credit information". The most important one concerns the very limit to disclosure, stating that "[c]redit information may only be given to persons that have an objective need for it" (1st para Section 4-3 PDR). Such a wording is one of the most important shortcomings of the entire chapter, for at least two reasons. First, the purpose remains rather vague, as it is not explicit what "an objective

[652] Regulations on the processing of personal data (Personal Data Regulations). Available at: http://www.datatilsynet.no/Global/english/Personal_Data_Regulations_20100215.pdf. Hereinafter: PDR.

[653] As stated in Section §1 PDA, the Norwegian data protection legal framework applies only to "natural persons".

need" can be, and how this can be validated[654]. "Objective need" is difficult to define without other elements, and the PDR does not provide more information, apart from in the Section 4-5, where it refers to Sections 34 and 35 of the PDA. Section 34 PDA obliges to "clarif[y] whether the processing of personal data may cause disadvantages for an individual which are not remedied by the provisions of Chapters II-IV [of the PDA, which define a series of rights of the data subjects and duties of the data controllers] and conditions pursuant to section 35". Section 35 PDA permits to "lay down conditions [in the licence] for processing when such conditions are necessary to limit the disadvantages the processing would otherwise entail for the data subject". Therefore, it is up to the Datatilsynet to carry on a sort of preliminary proportionality test on the types of processing foreseen by companies, and the same DPA has the power to insert specific conditions and limitations in the licence itself. The second reason is that the PDR does not oblige, explicitly, the enterprises providing credit information services to check the request they receive before for disclosing the information. Nothing in the legislation prevents companies, once the licence is granted, to not respond to queries on credit information that could be considered non-legitimate. They have no explicit duty to check if the requiring party has "an objective need" for the credit information. Therefore, there is no specific filter to ensure that data are not unduly disclosed, but only an *ex post* control based on the data access provision discussed below. This appears to be one of the most salient features of credit scoring as surveillance in Norway, the very wide access based on the vague definition of "objective need".

Based on our media analysis, we found that both the DPA and the major credit scoring agencies, such as DNB Nord and Dun & Bradstreet, appear to be challenged by this vague and wide definition. According to Dun & Bradstreet, the responsibility for ensuring that the credit check is valid lies with the clients buying their services[655]. This means that the

[654] As discussed below, the Datatilsynet plays an important role in the field, not only because of its general role as Data Protection Authority, but also because it is the agency entitled to grant licences to enterprises willing to operate credit information services (cf. Sections 4-5 and 4-7). It is at the level of the granting of the licence that the purpose for disclosing credit information is discussed.

[655] http://www.aftenposten.no/jobb/Tar-kredittsjekk-av-kjaresten-6616597.html#.UtZmUnmA2ig

responsibility for interpreting the legislation shifts from the credit scoring agencies and to the large number of clients performing credit-based services. The DPA has few ways of sanctioning the companies, other than letting them know what is considered the right practice[656]. It should also be noted that credit checks can be performed based on even a very small sum of money, making the possible scope of the practice quite wide. The DPA reports to have handled cases where sums as low as 200 NOK (approximately €23) have been considered as a sufficient risk for the credit providers, and hereby approved as an "objective need" for credit scoring[657]. Paired with the lack of obligation to check requests upon disclosure and the low limiting effect of the definition of "objective need", the responsibility and accountability of credit scoring is mostly shifted from the credit scoring agencies to their clients.

Section 4-3 PDR also establishes as a general rule that information should be "provided in writing", the oral communication being only an exception, to be "confirm[ed] in writing" in most of the cases[658]. This procedure can be considered a safeguard for the data subjects requiring access to credit, as it creates a substantial trace of the effective use and result of credit scoring.

Section 4-4 PDR does not only extend the right of access established in the main legislation (cf. Section 18 PDA) to this field of processing and to "legal persons". This provision also introduces a duty for credit information enterprises to "send a duplicate, copy or other notification concerning the contents" to natural persons (i.e. data subjects) when credit information has been provided about them (1st para Section 4-4)[659]. Furthermore, "[t]he data subject shall be invited to request that any errors be rectified" (1st para Section 4-4). This

656 http://www.dn.no/forsiden/article1676075.ece

657 http://www.dinside.no/875910/kredittvurderes-uten-grunn

658 A third form of disclosure is foreseen for business companies and under specific conditions: "distribution of publications or lists" (3rd para Section 4-3).

659 A similar approach to data access rights, shifting part of the burden on data controller, can also be found in the PDA in relation to the "use of personal profiles" (cf. Section 21 PDA), and is considered to be a peculiarity of the Norwegian data protection system, cf. Bygrave, L.A. (2002) *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague/London/New York: Kluwer Law International, pp. 332-334.

notification contains the kind of information provided about the person that has been assessed, the source of the information, who asked for the information (including address and phone number), and, if relevant, the name of the department or branch of the organizations asking for the information. Finally, the same provision further widens the data access rights of the data subject, as she can require "to be informed of what credit information has been provided about [her] in the last six months, to whom it was given and where it was obtained" (3rd para Section 4-4).

In theory, this Section is a key element of the entire Norwegian system. It provides a rather high level of transparency and ensures the awareness of the practices even when credit scoring is illegitimately operated. For example, the possibility of secret processing is practically inexistent, at least when this processing translate into disclosure of information. Furthermore, this provision potentially exposes illegitimate requests of disclosure, but only when they are fulfilled. However, Section 4-4 PDR is far from being the perfect solution in terms of awareness and transparency. As mentioned above, the copy of the disclosed data is only provided at the same time of disclosure itself, which practically means that there is no effective possibility for the data subject to oppose the release itself of her information in case of non-legitimate credit scoring. The only possibility is to complain *ex-post*, after the disclosure. Moreover, the awareness is not 'collective', in the sense that while each individual can become aware of the processing and disclosure of her own information, no clear picture of the size and main feature of credit scoring can be created. Indeed, the provision does not foresee the statistical aggregation of data on disclosure (e.g. how many, for which purposes…) or the publication of reports on the legitimacy of disclosures.

The second key element of credit scoring regulation is the ad hoc license system, administrated by the DPA. As mentioned above, the license system was already introduced at the time of the first Norwegian Data Protection legislation (cf. section 2.1 above). Following specific cases from *Personvernnemnda* and the DPA, the content of the licence was revised in a process started in 2009, and the final revised licence was finished in the

beginning of 2012[660]. The remainder of Chapter 4, Sections 4-5 to 4-7 of the PDR concerns this licence system.

Section 4-5 states that "[a]n enterprise may not process personal data for credit information purposes until the Data Protection Authority has granted it a licence". This obliges all enterprises willing to carry on credit scoring to seek not only a general permission, but a veritable licence, which clarifies and limits, *inter alia*, the sources of data to be used, the different processing operations for different categories, the rules on the storage of information and data in specific registers. This licence-based system further strengths the powers of the Datatilsynet, which is the only authority that can grant the licences (1st para Section 4-5), and that can also "exempt the data controller from obligation[s]" derived from the same Chapter 4 (Section 4-7). Also, it is possible to state that each specific licence (based on a common template)[661] becomes a sort of *ad hoc* data protection legal instrument.

The general licence application for the processing of personal data[662] contains several requirements to be fulfilled, and is only an orientation from the data controller to the DPA, and no manual approval is given from the DPA[663]. Once the licence for processing personal data relating to credit scoring activities is given, the company receives a letter from the DPA stating more clearly the rules for the practise and what the register can contain. According to Section §35 PDA, several requirements must be met. The register can only contain certain kinds of information, and this information is divided between information concerning data subjects and legal subjects, and also between credit information obtained from public and not-public sources. Some kinds of information are merely basic data concerning name (of data subject or legal subject), contact information and organisational number, whilst other types of information remain more vaguely defined: "commercial interest" (for data subjects)

---

660 The main changes and controversies related to the license system are described in section 3.2 below.

661 The basic template is available online on the website of the Datatilsynet: cf. http://www.datatilsynet.no/Global/05_regelverk/Konsesjoner/Konsesjon_kredittopplysning_2012.pdf.

662 In Norwegian: Søknad om konsesjon for behandling av personopplysninger i henhold til personopplysningsloven (pol.) §33 og personopplysningsforskriften (pof.)

663 http://www.datatilsynet.no/personvern/Melding-og-konsesjon/

or “actual events of a natural and economic character that obviously matters” (for legal subjects). The DPA also states requirements concerning the sources from which personal data can be obtained. They generally include phone companies, media, other credit scoring agencies, Statistisk Sentralbyrå (SSB)[664] and other public registers. Notably, the public tax lists, *Brønnøysundregistrene*[665] and Norsk Lysningsblad[666], are among the public registers whose data may be collected[667]. Further requirements concern also the process of actual disclosure, including the obligation of not marking ex post notifications with the company logo, and of using the fastest form of postage possible[668]. The license also includes specifications about “objective need”, the possibility for “credit freeze” and the adequate routines for erasure.

2.3 The main credit scoring practices

Credit scoring in Norway is seemingly considered quite a natural practice. One of the largest credit information enterprises calls credit scoring “an everyday shopping item in a consumer society”[669], which could be further interpreted as a sort of *on-demand surveillance*[670]. The legal access to credit scoring a natural person is limited to actions where goods or services are purchased and there is an element of credit involved. Applying for loans or credit cards, requesting to sign up for a phone or television contract has been named as such examples. A list of practices not legally considered credit scoring is provided in Section 4-2 PDR, including for example notifications from public registers regarding rights in and charges on

[664] *Statistics Norway*. www.ssb.no

[665] The Brønnøysund Register Centre is a government administrative agency responsible for a number of national regulatory and registration schemes for business and industry.

[666] Norsk Lysningsblad is is an online publication of public announcements such as debt negotiations and remaining debt of a deceased.

[667] It should be noted that setting up a credit block or credit freeze is not considered as public information.

[668] When browsing the websites of the largest credit scoring agencies in Norway, we note that the use of electronic notifications seems to be of increasing use.

[669] http://soliditet.no/vaare-tjenester/kredittsjekk/kredittsjekk-person

[670] Even though a credit check is a service you can buy, none of the large credit scoring agencies focused on in this report has any information about the price of their services on their websites.

real or movable property, and notifications from banks and finance companies. As previously mentioned, credit-scoring practices concern both natural and legal persons, with the result that the scope of data protection in relation to credit scoring is extremely wide[671].

A classical example of the workflow of credit scoring is the following: an individual wants to purchase a service including credit, i.e. setting up a cell phone subscription. She signs a contract with her name, national ID number, address etc., agreeing to the relevant terms and conditions. The latter include the possibility to carry on a credit check on the prospective cell phone subscriber. Then, the credit provider (in this case, the phone carrier company) uses the services of one of the licensed companies to obtain the credit score of the individual. No matter the outcome of the credit check, the prospective customer (the data subject) receives a notification by mail or email including the information that the phone carrier company received from the credit scoring agency. If the notice to the credit provider comes with the conclusion that nothing negative is registered on her, or with a score that is deemed appropriate by the credit provider, the cell phone subscription is put into action. Otherwise, the credit is denied (in this case, the mobile phone subscription). If the subscription is denied, or the data subject notes errors in the information that has been provided by the credit scoring agency, she can complain to the same, and, if deemed necessary, to the Datatilsynet.

To this date, eleven enterprises are given a license from the DPA for credit scoring[672]. Norske Kredittopplysningsbyråers Forening (NKF) (Norwegian credit scoring agencies union) is an umbrella organisation organizing the major credit scoring agencies, but it has proven difficult to obtain any further information on this organisation. Soliditet Decision, one

[671] Shartum Wiese, D. (2001) Norway. In *Nordic Data Protection Law*, edited by Peter Blume, pp. 79-113. Copenhagen: DJØF Publishing. In this report, we limit our focus to credit scoring practices and controversies concerning individuals.

[672]According to the website of the DPA, (per 16.01.2014) these are: Experian, Bisnode Credit AS (formerly known as AAA **S**oliditet AS, Atradius buyer Ratings, Kredittopplysningen AS, KO International AS, Soliditet Decision and Nordic Insurance Services.

of the eleven, has performed credit scoring for over a hundred years[673], and offers a brief description of its main services. When it comes to credit information on individuals, Soliditet Decision uses a database "contain[ing] information about approximately 4.2 million Norwegians".[674] Everyone with taxable income is registered with the credit information agencies[675]. The kinds of information contained in the database are pretty diverse: "basic personal data, Decision Score Person, tax assessment (past three years), estimated gross income, name and address history, business interests, non-payment records and any security furnished voluntarily".[676]

The Decision Score Person is among the most interesting types of data, because it is the fruit of the processing of other data by the company itself, and because it somehow synthesizes the overall credit score by ranking individuals according to a predicted risk of default.[677] According to their website:

> Decision Score Person tells you in a simple and user-friendly manner which customers have a high, medium and low risk of default. On the basis of extensive analyses, we have identified the most important variables that best predict the likelihood of a person defaulting on commercial credit (non-payment record or debt collection) during the next 12 months. These variables, by themselves or in combination, decide which zone a person belongs to. In addition to the statistical likelihood of defaulting on commercial credit, we also employ a set of overriding policy rules that may affect the decision to grant credit.

Soliditet Decision uses a scoring system with points ranking from 0 to 100, where the points indicate how creditworthy the data subject is. The higher the number, the less likely the data

---

673 The major expansion of Soliditet in Norway however, took place in 1984 when the Norwegian part of Soliditet was sold to Esselte, leading to several acquisitions. At the end of 1986/ 1987, the central register for credit information was merged with Soliditet, and the two beta bases could be merged. https://www.soliditet.no/om-soliditet/hvem-er-soliditet

674 https://www.soliditetd.no/en/products. The total population of Norway reached five million in 2012.

675 http://www.regjeringen.no/nb/dep/bld/dok/regpubl/prop/2012-2013/prop-195-l-20122013/6/1.html?id=736122

676 *Idem*.

677 *Idem*.

subject is to get payment problems later on. A score of 19 means for example that there is a 3,5 % chance of the data subject to get a non-payment record in the next 12 months, in other words there is a 96,5 % chance of a successful relationship between the data subject and the credit provider. Usually, a score of 18 or higher is considered a positive result by the costumers of Soliditet Decision, but this number will vary according to the type of risk the credit provider company is willing to take or to different credit policies. The risk is also categorized in five zones: zone 1 (high risk), zone 2 (moderate risk) and zones 3 to 5 (low risk). The score model serves only as a decision support, as the final decision lies with the credit-granting entities. Soliditet Decision lists a stable income as the safest way for the data subject to improve the credit score, and a non-payment record as the specific fact influencing your credit score in the most negative way[678].

Another major actor in the field of credit scoring is Experian Credit Services[679]. The databases of Experian combine public accounting with credit information from various sources, such as the country's debt collecting agencies. Experian uses three different models for credit scoring, each basing its score on various elements. "Risk Score Person" measures the data subject's present economic state, and is not a predictive model. "Consumer Delphi, generation 1" measures the probability of the data subject getting a non-payment record (*betalingsanmerkning*) during the next 12 months, and is therefore a predictive model. Both of these models score the data subject from between 0 to 100, where 100 indicate the best creditworthiness. "Consumer Delphi, generation 2" is the newest predictive score model of Experian, based on nine different industry-specific models, acknowledging that enterprises from different industries require different kinds of credit, and that the risk related to the various groups will vary between industries. This model also

[678] No single action can in itself decide the final credit score, but some actions have a larger influence than others. One example of a strategy that could work both ways is applying for a higher credit limit. http://money.msn.com/credit-rating/should-you-increase-your-credit-limit

[679] http://www.experian.no/om-oss/credit-services.html

measures the probability of the data subject getting a payment record during the next 12 months, but uses a scale ranging from 0 to 1000[680].

As already mentioned, all companies providing a service involving a credit can require credit information on the individual willing to sign the contract. Beside legitimate (regulated) uses, credit scoring can be considered a particularly pervasive practice because of the potential non-legitimate uses, linked to the weakness of the regulation when it comes to ex ante controls (cf. section 2.2 above). While we discuss some of the non-legitimate uses and abuses in the following sections, it is important to note that they also include individual-to-individual relations, and not only company-to-individuals one. The examples provided on the website of the Norwegian DPA include those of former partners wishing to collect information during the separation and divorce cases, as well as those of landlords wishing to verify the ability to pay of prospective tenants[681]. A strategy for avoiding credit scoring is to set up a "credit blocking" ("credit freeze", or "kredittsperre" in Norwegian). The DPA provides you with a template if you wish to contact the credit scoring agencies to set up a credit block[682], and they also list the addresses of the three most common credit scoring agencies (Bisnode AS (including enterprises such as AAA Soliditet), Experian AS and EVRY AS)[683]. The use of this strategy is increasing, and the number of Norwegians setting up a credit blocking is tenfold in the last five years[684]. The backside of such a blocking is that several other possibilities are blocked as well, such as applying for loans or engaging in the many mundane tasks that

[680] http://www.experian.no/kundeservice/p-faq-kredittscore.html

[681] This kind of individual-to-individual practices (or abuses) of credit scoring are also mentioned in the website of the Datatilsynet, as reasons why some data subjects may want to consider to require a blockage to credit scoring: cf. http://www.datatilsynet.no/verktoy-skjema/Sporsmal-Svar/?qlist=1654,1653,614,601,603,607&question=1654&ref=1652 (last accessed 13.06.2013, in Norwegian only). It is not clear if credit information collected non-legitimately can be used in courts, for example in a cause for divorce. The Datatilsynet official that we interviewed was not aware of any major case law in this specific field, but pointed to the fact that there has been at least one important judgment where the Supreme Court accepted evidence collected with infringement to data protection law, arguing that the infringement was to be balanced against the issues at stake in the overall case. ADD REF.

[682] http://www.datatilsynet.no/Sektor/Kreditt-finans-forsikring/Hvordan-sperre-for-kredittvurdering/

[683] The information in this section is gathered from the website of the DPA.

[684] http://www.dn.no/privatokonomi/article2203446.ece

involve credit. Hence, and somehow paradoxically, the set up of a credit block highlights how comprehensive the practise of credit scoring has become in Norway.

Even though this practice could be interpreted as a strategy of resistance, it most saliently appears to be a strategy for self-governance or self-discipline, shifting the focus from the problems with the practice to the problems with the self. According to our media analysis, the reasons for setting up a credit block can be manifold. For example, it permits to avoid ID theft, since a common way to commit identity theft is to raise a credit in the victim's name. Another reason can be to put limitations to personal consumption, limiting the ability to order credit cards and contract credits[685]. To avoid unnecessary credit and "snooping" is another reason[686]. Employees of companies that have access to credit information (employees of banks, financial institutions, and companies with agreements with credit information agencies) can use the access to things other than just checking customers. The DPA reports of having received a number of cases where people have been credit checked during courtship, child custody and divorce[687].

3 Controversies

3.1 Media coverage of credit scoring controversies

Based on our analysis of Norwegian media coverage of credit scoring over the last decade, few controversies have emerged[688]. The controversies can be divided into different categories: (i) the misuse of credit checks with the wrong intentions; (ii) non-

[685] A report by SIFO, The National Institute for Consumer Research, about Young Adults and Credit-Financed Consumption, confirm that young adults wished that credit and credit cards were much harder to obtain, and that the aggressive marketing (in shopping centers etc.) is very negative. One of the interviewed even made the comparison to alcohol and tobacco, stating that if advertising such items are forbidden, then credit cards should be as well.

[686] According to an interview with Director of Analysis in Experian, Bente Thorbjørnsen, "rich people wants to avoid snooping and fraud, while the indebted wants to avoid any more credit debt"; cf. http://www.dn.no/privatokonomi/article2203446.ece

[687] http://www.dn.no/forsiden/article1676075.ece

[688] The main media taken into consideration has been the newspapers *Dagens Næringsliv* and *Aftenposten*, which is two out of four of the largest in Norway, and the online consumer oriented news site, *Din Side*. From the other two newspapers in the top four, *Verdens Gang* and *Dagbladet*, not a lot of inside was gathered.

legitimate/unnecessary credit scoring; and (iii) identity theft. The first appears to be the most prominent category. In connection to an article from 2011, 55% of the respondents in an online questionnaire reports to unrightfully having been credit scored.[689] Despite this high percentage, in our analysis of the media coverage, we have not found any particular case in which the triviality or the pervasive nature of credit scoring itself is being criticised. This seems to point to the fact that the practice of credit scoring does not seem to be controversial in itself. What is often at the forefront of debates is the possibility of non-legitimate credit scoring.

The most prominent controversies concern the use of credit scoring for other reasons than the legislation allows. In this sense, the key debate is the case of rental brokers' access to credit scoring prospective tenants. This is an example where the same action (to credit score prospective tenants) is legal for some actors and illegal for others based on the notion of manageable financial risk. In 2009, the marked leader in home rental real estate in Norway, *Utleiemegleren*, were initially refused to credit score prospective tenants based on the fact that they should be capable of handling the financial risk[690]. They filed a complaint on the decision, and the refusal was later reversed by the Privacy Appeals Board[691]. The rationale behind the Privacy Appeals Board's decision was based on the considerable size of the company in the market and the fact that the people renting out their apartments and houses through Utleiemegleren were private people who could not be faced with the economic risk that companies could[692]. If Utleiemegleren had been a professional rental broker who owned properties and rented them out, the decision would be different based on the fact that the economic risk would be considered a natural part of normal business practice, and credit scoring would be illegal. To sum up, for natural persons it is admissible to credit score

689 http://www.dinside.no/875910/kredittvurderes-uten-grunn

690 http://www.regjeringen.no/nn/dep/kmd/Dokument/proposisjonar-og-meldingar/stortingsmeldingar/2009-2010/meld-st-5-2009-2010/7/7.html?id=579021

691 http://www.personvernnemnda.no/vedtak/2008_1.htm

692 *Ibid*.

prospective tenants given the eventual economic risk, but it is not admissible for professional rental brokers because the eventual economic loss could be easily pulverized[693].

The controversy concerning the credit scoring of prospective tenants is also interesting because it highlights the trends towards further use of credit scoring. According to an officer in the DPA interviewed in 2007, the fact that smaller rental brokers inform about the credit scoring of tenants does not change the fact that it is illegal: "Getting consent doesn't change the legislation"[694]. The DPA officer points to a decision by the Privacy Appeals Board in 2006 which, after receiving a complaint from the DPA about a large company performing unnecessary credit scoring on tenants, refused this credit scoring practice because it were considered a normal risk[695]. This prohibition was interpreted by some actors as an opening to create a credit element in the rental agreement, so to fulfil the legal requirement for credit scoring. This can for example be done by moving the due date for the lease for new tenants towards the middle of the month, resulting in part of the rent being paid arrears[696]. These two cases seem to have become a sort of case law on this specific field of conflict, one resulting in denial and the other giving access.

The second set of controversies concerns abuses. A specific type of abuse concerns people employed within institutions performing credit scoring for personal advantage, e.g. for dating or relationship purposes, for influencing divorce settlements in relation to the sharing of finances and costs, or cases of child custody – to prove to be eligible to take care of a child[697]. The misuse of credit information for such purposes are, according to an officer in Bisnode, a rather "on the verge of being idiotic", since every employee who has access to the search functions in the system has to log in with their personal identification, leaving

[693] http://www.datatilsynet.no/verktoy-skjema/Sporsmal-Svar/?question=1963&qlist=1792,201,599,600,601,603,604,605,606,607,608,609,611,614,1653,1654,1963&tema=12

[694] Cf. http://www.siste.no/Innenriks/article2922553.ece

[695] Cf. http://www.personvernnemnda.no/vedtak/2006_3.htm

[696] Cf. http://www.noeiendom.no/article.php?articleID=135&categoryID=6

[697] Cf. http://www.dn.no/forsiden/article1676075.ece

clear traces back to the responsible[698]. DnB Nord goes even further, and states that such abuses are considered a reason to fire the responsible employee.[699]

Within the same set of controversies, another debated issue in the media is the credit scoring of job applicants. In this case, it remains a bit unclear as to whether or not this is an acceptable practise. Concerning the legal demand for "objective need" for credit scoring[700], this seems to not always be the case. The DPA states that the rules for credit scoring a job applicant are very strict, and they list three criteria[701]. First, it has to concern a high position in the hiring institution. Second, the position has to include financial management. And third, credit scoring is only allowed on applicants in the final stages of the process of hiring[702]. However, there seems to be no clear practise as to how these requirements are fulfilled on a regular basis. This particular statement was given in relation to a case where professional chauffeurs of long-distance transportation protested against a company credit scoring, by default, all job applicants. The rationale of the systematic credit scoring was based solely on the fact that prospective employees were to handle money, and thus their 'financial moral' had to be checked. The DPA concluded that this particular practise did not fall under the criteria listed, and stated that even if the job applicants had consented to the credit scoring, the practice would still not be considered acceptable[703].

For the last category of controversies, the emerging issue in the media includes identity thefts leading to unwarranted credit checks. When searching online for media coverage on credit scoring in Norway, a substantial amount of hits concerns identity theft. Many cases

---

698 Cf. http://www.nettavisen.no/okonomi/privat/article2633566.ece

699 Cf. http://www.nettavisen.no/okonomi/privat/article2633566.ece

700 As described in the previous section concerning the legal provisions of credit scoring.

701 http://www.datatilsynet.no/verktoy-skjema/Sporsmal-Svar/?question=201&qlist=1792,201,599,600,601,603,604,605,606,607,608,609,611,614,1653,1654,1963&tema=12

702 The result in this particular case was that chauffeurs of long distance-transport, did not fall under these criteria. Cf. http://www.transportarbeider.no/kunder/ntf/cms.nsf/($All)/747B6854916FF21DC12578A000371465?OpenDocument

703 Cf. http://www.transportarbeider.no/kunder/ntf/cms.nsf/($All)/747B6854916FF21DC12578A000371465?OpenDocument

revolve around criminals obtaining information about the subject's personal data, and making credit purchases, leading to unwarranted credit checks of the identity theft victim. For example, one case included a credit card being stolen from a mailbox, leading to 42 different new phone subscriptions being made in the victim's name, an action requiring the phone companies to perform a credit check[704].

Apart from these sets of controversies, our media analysis highlighted other two relevant themes. On the one side, several media cases underline the fact that the blocking of credit checks is an increasing trend (cf. section 2.3 above)[705]. However, it does not seem that the diffusion of such a strategy relates to fundamental issues with the credit scoring itself, but rather to a need of self-discipline of individuals. For example, *Gjeldsofferalliansen* – the Norwegian Organization for victims of debt – recommends setting up a credit block and not requiring credit cards and credit loans as a strategy to limit own consumption[706], calling it a form of voluntary blacklisting yourself[707]. On the other side, the theme of being excluded from services relying on credit has been raised also in relation to people living on boats[708]. In this case the 'blacklisting' is not voluntary, but a side effects of the fact that these individuals are not registered in *Folkeregisteret* - the public address database - and they are defined as "homeless" by i.e. the tax authorities. Therefore, they cannot get credit checked, and they miss out on benefits of loans etc. Some cases concerning the denial of credit services were debated in the media in the summer of 2013, with the result that the tax authorities decided

[704] Cf. http://www.tv2.no/nyheter/innenriks/neddynges-av-fakturaer-etter-idtyveri-4073229.html#.UtPoEXmA2ig. The Norwegian police reports that approximately 2000 new phone subscriptions are made every year using false ID. http://www.eikernytt.no/nyhet.cfm?nyhetid=8773

[705] http://www.dn.no/privatokonomi/article2203446.ece

[706] *Gjeldsoffer-Alliansen* (GOA) is an organization by and for victims of debt. GOA was formed in 1991, and has approximately 700 members. GOA goal is to spread information and help people who have fallen under a debt they no longer can handle. As part of this information campaign, they encourage members to credit score themselves, and they provide links and forms to make this easy.

[707] 'Blacklists' were published by several credit scoring agencies in the 1970's. NOU 1974: 10: 11.

[708] http://www.osloby.no/nyheter/---Vi-foler-oss-ikke-som-uteliggere-7245316.html#.UxcBO0aYaig

to change the practice, including boat-inhabitants within the same legal framework as others[709].

3.2 Complaints concerning credit scoring

As already emphasized above (sections 2.1 and 2.2 above), Norwegian data protection legislation and credit scoring practices are deeply entangled. Therefore, it is not surprising that most of the formal complaining is channelled via data protection, and in particular via the engagement of data protection institutions: the *Datatilsynet* and the *Personvernnemnda*.

When it comes to data protection issues, contacting the DPA is generally considered the first step for data subjects considering lodging a complaint. From the annual reports by the DPA, we can read that in 2010[710] the DPA handled around 1600 cases, mostly from natural persons, asking if the PDA had been respected in different cases. Use of CCTV, disclosures of full birth number and credit scoring were the main themes. Regarding the latter, the issues at stake concerned mainly data subjects not being able to understand why credit scoring was necessary in specific cases, or not understanding why they had been subject to credit scoring at all. Thus, similarly as it was the case for the controversies in the media, most of the issues and complaints coming from data subjects focus on illegitimate disclosure, rather than radical opposition to credit scoring.

From 2009-2011 the work of revising the credit scoring license was carried out[711]. Among the reasons for the revision was the misuse of credit scoring to bully, based on an assumption that financial data could be sensitive and worthy to protect, even if they were not sensitive by the letters of the law. Another reason was that the parameters used by the credit scoring agencies are somewhat dubious, based on the fact that parameters like age, sex and address can lower your credit score even if you have not had one record of bad

709 http://www.osloby.no/nyheter/--Supert_-da-har-vi-vunnet-saken-for-mange-batbeboere--7245747.html#.UtUHuHmA2ig

710 http://www.datatilsynet.no/Global/04_planer_rapporter/aarsmelding/aarsmelding_2010.pdf

711 The information on this paragraph is taken from the Annual Report of the DPA for 2012. http://www.datatilsynet.no/Global/04_planer_rapporter/aarsmelding/%c3%85rsmeldingen2012.pdf

payment. The new licence was a result of collaboration with the credit scoring companies, and the reason for the revision was a number of cases from Personvernnemnda and the DPA. The new license was official since 1st of April 2012. Some parts of it were issues to complain, i.e. *Norske Kredittopplysningsbyråers* forening complained about the refusal to use address history as a parameter. The revision also suggested a common register for reservations against credit scoring, and to create a standard response letter to use for complaint to credit scoring agencies. Other debated issues following the revision were the use of the number of previously performed credit scores as a parameter, property ownership, and information about invoices settled prior to due date[712].

The DPA annual report from 2011[713] raises an interesting issue, stating that within the bank industry, there are new companies emerging with the aim of developing techniques for profiling peoples credit worthiness based on their activities and networks in social medias. A Norwegian article from the same year calls the phenomena "social credit scoring"[714]. We have not been able to find evidence of these practises being carried out in Norway, but the fact that the DPA raises the issue in their report can maybe tell us something about the prospective development. The report from 2011 also describes the increasing trend of gathering more data for assessing the possibility to offer insurance and its conditions[715].

The DPA plays also a more proactive role, as it provides on its website a template for lodging a complaint to the credit scoring agency at stake[716]. This practise may serve to highlight even further the important function of the DPA with regards to credit scoring practises in Norway, and the mutual entanglement of data protection and credit information services.

---

[712] According to the DPA report of 2011, Personvernnemnda handled complaints regarding these issues again in 2012, and the new decision allowed for using information about if *legal* persons had settled their invoices before due date. Ownership to property was approved for natural persons as well. Address history however, was not approved.
[713] http://www.datatilsynet.no/Global/04_planer_rapporter/aarsmelding/aarsmelding2011.pdf
[714] http://www.dagensit.no/article2293846.ece
[715] Annual Report of the DPA for 2011: p. 53
http://www.datatilsynet.no/Global/04_planer_rapporter/aarsmelding/%c3%85rsmeldingen2012.pdf
[716] Cf. http://www.datatilsynet.no/Sektor/Kreditt-finans-forsikring/Klage-pa-kredittvurdering1/

When a case (either from a legal or natural person), leading to a decision at the DPA, is subject to complaint, the Privacy Appeals Board decides appeals against decisions. The *Personvernnemnda* is a Norwegian *sui generis* institution, which acts as an "independent administrative body subordinate to the King and the Ministry" that "shall decide appeals against the decisions" of the Datatilsynet (Section 43 PDA). While its decisions cannot be considered judicial case law, they have an important impact of the interpretation of data protection law, and, in specific cases, on the possible shaping of surveillance practices. Few cases directly concern credit scoring practices. Below, we briefly describe some of these cases.

A joint complaint in 2012 by several credit scoring agencies' requested to add new sources of data to their existing pool[717]. In this case, Personvernnemnda partly took the appeal into account, by including two out of four disputed sources of information in the license.

In 2010 the Privacy Appeals Board received a request for reversal on a decision regarding insurance companies' access to credit scoring information[718]. The request for reversal relates to a proposal for modification of Section §4 of the general licence (concerning the processing of personal data for credit scoring purposes). The demand of change aimed at allowing the use of credit information in the risk analysis carried on by insurance companies. The request for reversal was not sustained.

In 2009, a request by journalists concerned the possibility to access credit scoring information as part of research for a television programme about consumer rights[719]. The complaint was not sustained.

In 2009, the DPA imposed changes on the duplicate letters/ex post notifications from three of the major credit scoring agencies. The goal was to allow data subjects not only to know about the fact that they had been objected of a credit scoring, but also about the actual

[717] Cf. http://www.personvernnemnda.no/vedtak/2012_07.htm
[718] Cf. http://www.personvernnemnda.no/vedtak/2010_6.htm
[719] Cf. http://www.personvernnemnda.no/vedtak/2010_1.htm

score that was attributed to them[720]. The three credit scoring agencies complained, but the complaint was not sustained.

A case from 2009 regarded the scope of the powers of the Norwegian DPA vis-à-vis credit scoring agencies' access and processing of specific data sources[721]. The judgment was triggered by a complaint by a company sorted in the highest category of risk based on the fact that they recently changed their daily manager of the company. Following, the complaint had to do with the weighing of the information from different sources. The DPA concluded that neither the PDA, the PDR nor the general licence regulates the weighing of the various information that credit scoring companies can legally obtain. The DPA concluded that they did not have the competence to assess the weighing of the different factors, and this remained the responsibility of the credit scoring agencies. The Personvernnemnda upheld the position of the DPA and the complaint was not sustained.

For the consumer's point of view, we studied the websites of the *Forbrukerrådet* – the Norwegian Consumer Council[722]. The Council is warning, especially young people, about the dangers of credit financed consumption, and offers advice on how to handle it. They point to some cases concerning minors receiving invoices for services they claim to have never used, i.e. porn sites. Another case is the "default" inclusion of credit cards in 'student packages' from banks. The Council stresses that requiring a credit card should be subject of actual need, and also that extra attention is needed to make sure that the regulations for credit services are followed. Given the high frequency of credit scoring and its pervasive role when it comes to everyday services, we expected the Consumer Council to be, by default, the main instance dealing with complaints about credit scoring. However, the Norwegian Consumer Council appears more kin on providing advice on how to lower the frequency of credit financed impulsive consumption, than on voicing complaints of individuals or carry on advocacy about credit scoring practices.

[720] Cf. http://www.personvernnemnda.no/vedtak/2009_1.htm
[721] Cf. http://www.personvernnemnda.no/vedtak/2009_2.htm
[722] Cf. http://www.forbrukerradet.no/forside

3.3 The tensions among the stakeholders

The analysis above of the sites and themes of controversy permits to advance few remarks not only on the co-constitution of data protection and credit scoring, but also on the diverse relations among key stakeholders. First of all, the main stakeholders in the field appear to be:

- the companies that have received a licence to provide credit information services. These companies are a bit diverse among them: some are only Norwegian while others are the Norwegian representatives of international companies. Some of them mostly focus on credit scoring-like activities, while others provide also different services (e.g. banking and insurance);
- the *Datatilsynet*, who plays a key role because it is in charge of granting licences to enterprises willing to provide credit information services, and it is also in charge of the overview of the compliance of the terms of the licences;
- the *Personvernnemnda*, which handles appeals against the decision of the DPA, and thus may participate to the shaping of the credit scoring practices (e.g. by allowing new data sources, or granting permission to operate credit check to new actors);
- private companies that are entitled to require credit information about customers. Given the possibility to carry on credit scoring also for small amounts of credit, this type of stakeholders may involve very different entities, from those that have credit as the main core business, to those that offer credit only as part of their services (or indispensable condition to access their services);
- companies that would not be entitled to require credit information about individuals but either attempt to do so (by asking formal permission to the DPA or consent from prospective customers or employees) or do so as part of their everyday practice;
- the data subjects (perspective credit customers) on which specific queries are done, and information on credit is disclosed;

- the data subjects on which queries are done without them being aware of, at least till reception of the *ex post* notification;
- the data subjects whose data are collected in the companies' databases. In the case of Norway, this implies the wide majority of the active population and any other individual who is registered in relevant national databases;
- the data subjects that make a request to credit score other data subjects;
- the consumers' associations, i.e. the *Forbrukerrådet*, which remains a relatively smaller player.

While at least three macro-categories could be indentified – the public authorities, the private companies, and the individuals – this division does not seem satisfactory as all of them play different roles. For example, the individuals, or data subjects, can be both considered 'watched' (when credit scoring is operated on them) and 'watcher' (when they require to operate credit scoring on someone else). In other words, access to this surveillance practice is not consistently or even formally prevented to them. Furthermore, data subjects themselves – through their data collected in national registers and their tracked behaviours, are the condition of possibility of credit scoring as a practice.

Even more interestingly, controversies do not always clear cut between watchers and watched, but even within the same category. For example, insurance companies have required access to credit scoring arguing, *inter alia*, that some competitors may already have access to this information. Finally, while the data protection public authorities – the DPA and the Privacy Appeals Board – are difficult to sit in the dyad watchers/watched, they definitely play a key role both in the deployment of the surveillance practice and in its eventual questioning. And, again, controversy can emerge between the two, e.g. when the Privacy Appeals Board reverses a decision of the DPA.

4 Conclusions

Based on our analysis, we can sketch a few specific features of credit scoring practices in Norway. First of all, nowadays credit scoring is a rather trivial and widespread surveillance

practice. It is a rather common experience for many people living in Norway and wishing to access not only credit in itself, but also other services premised on credit. Thus, even the subscription of a mobile phone contract can become a legitimate occasion to undergo credit scoring.

Credit scoring functions as a sort of on-demand surveillance practice: only few companies can operate the credit check in itself, but many diverse actors may request and pay for this service. While private companies are among the main users of this service, our analysis has shown that there are also cases of individuals asking for credit scoring of other individuals, for example for assessing the solvability of prospective tenants, before dating someone or in cases of divorce causes. The main barrier to operate credit scoring is the principle of "objective need" established by data protection law, but it does leave the access wide open, as the credit scoring companies have no obligation to verify it.

While credit scoring can be considered a mundane experience for many individuals, awareness is formally built into the practice itself: both *ex ante* and *ex post* the credit check. Generally the person requiring a service has to consent to be credit checked before the service provider can send a request to one of the credit scoring companies. Then, after the credit check is carried out, the credit scoring company has to send a notification to the person at stake. This latter operation is mandated by law, and ensures that even illegitimate credit scoring is notified to the relevant data subjects (with the potential exception of abuses by credit scoring companies' employees). Compared to other surveillance practices involving forms of profiling, the *ex post* notification system is a specific feature of credit scoring. Still, in cases of illegitimate requests of credit scoring, this sort of 'awareness by design' cannot prevent disclosure, and only permits to data subjects to complain after surveillance has taken place.

Credit scoring practices are not only pervasive in terms of availability and effective use by diverse actors, but also for their material constitution. Credit scoring companies have to build pretty extensive databases to both carry on their analyses and create their risk profiles.

Therefore, individuals are not only the objects of credit scoring, or the entity requiring assessment, but they alsoparticipate – through the translation of their behaviour into personal data – to the effective making and evolution of the surveillance practice. Given that credit scoring companies have legal access, *inter alia*, to some national public registers (e.g. *Brønnøysundsregistrene*), this means that practically all active individuals working in Norway are, willing or not, embraced by this form of surveillance.

Access to national public registers highlights the strict relations of credit scoring not only with the economic system, but also with the state and the public administration architecture. The entanglements with the public become even more evident when it comes to data protection legislation. At least since the 1970s, the evolution and deployment of credit scoring has been accompanied by the development of the Norwegian data protection legislative framework. The interactions with data protection are not merely a question of limitation and channelling, but rather of proper co-constitution. The Credit Information Committee proved to be highly influential in the drafting of the first Norwegian data protection legislation. Then, data protection regulations became the legal basis to carry on credit checks, creating a *sui generis* legal framework that includes specific provisions and rules, and an *ad hoc* licence system. In many senses, the Norwegian DPA and the Privacy Appeals Board do not only ensure the protection of the rights of data subjects, but they also contribute to morph the conditions of possibility of credit scoring. For example, the licence system grants a key role to the Datatilsynet, which is responsible for granting new licences and enforcing their conditions.

The strict relation between credit scoring and data protection is also evident when analyzing the main controversies emerged during the last few years. Rather than being framed through consumer law or via consumers' protection institutions, most of them are channelled through data protection instances. Generally, complaints are firstly routed to the Norwegian DPA. The decisions of the DPA can be appealed to the Privacy Appeals Board, and in this venue

important decision about the functioning of the credit scoring system, or access to their services, have been taken.

Beyond the hegemonic role of data protection, the analysis of controversies has shown other two interesting aspects of credit scoring in Norway. On the one side, there is no formal collective opposition to this surveillance practice. In none of the cases identified, credit scoring as such was called into question, but only specific uses and abuses (e.g. the credit scoring of prospective tenants or job candidates). So, even if there are several complaints, they remain somehow atomized and very punctual. Surely, some cases brought to the attention of the Privacy Appeals Board have far reaching consequences, for example those concerning access to specific data sources or the possibility for insurance companies to carry on credit checks. However, the existence of the practice is never formally called into question.

On the other side, a potentially radical form of opposition to credit scoring is not only available but also institutionally publicized by key stakeholders: the so-called *kredittsperre*. Individuals can formally prohibit credit scoring agencies to check them, and thus to never accept demands to do so from third parties. Even if they do not formally or institutionally question the surveillance practice in itself, they oppose to it in a pretty radical way: they opt out and limit its reach. As access to credit-related services is no possible anymore, a credit blocking emphasizes and exposes the pervasiveness of credit scoring and its embedment and impact on everyday life.

Playing the System and the Fight Back

- Credit Scoring in the UK

'Credit is part of the ebb and flow of social life, for nobody is or can be or should be truly self-sufficient' [723]

[723] Williams, B. (2011). *Debt for sale: A social history of the credit trap*. University of Pennsylvania Press. (p.5)

1. Introduction

In December 2012 the New York Times ran an article about how even Cupid has an interest in credit scores.[724] As the Times explained for a couple on a date the awkward etiquette of when to ask 'how is your credit rating' inevitably arises. While the question may seem crass and preposterous to several audiences, the practical implications of the question to some New Yorkers have consequences that they simply want to know about. If a person has poor credit, there are potential financial implications for the blossoming relationship; for example the negative effect a poor credit rating would have if the couple where to buy a home together. The New York example goes someway to highlighting the societal impact credit scoring is inducing in how we now live our lives. Financial capacity it can be argued has always played a role for Cupid (just think of how dowries work) and for some it may seem strange that it has taken this long for credit rating to come to the fore in the 'dating' world. However, what may be more startling is the growing prevalence and influence of this type of rating system. As Lyon has argued 'social sorting' is a distinctive feature of the surveillance society and credit scoring gives a very real example of how this effect is taking place.[725] Your score sorts you out; it highlights your capability of securing credit. Within various societies credit is an extremely important vehicle in enabling betterment or even survival; credit secures loans to buy homes, to start businesses or even pays the gas bill until the next pay-check arrives. Gaining access to credit is important for the lives of many.

This report looks at credit scoring in the UK and examines two trends: 'playing the system' and the 'fight back'. The first refers to how consumers may be using the credit scoring system to their advantage, especially when faced with problems such as the refusal of

[724] http://www.nytimes.com/2012/12/26/business/even-cupid-wants-to-know-your-credit-score.html?_r=0

[725] Lyon, D. (Ed.). (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Routledge.

credit.[726] Citizens avail of information, mainly sourced online, in how they deal with the issues that prompted their rejections. The second trend looks to a credit product – pay day loans – and examines how organisations selling this product have encountered hostility from the media, and governments, due to the unscrupulous nature of their business models. What links these trends is their resilience in the face of difficulties, as well as the fact both trends involve information being processed, analysed and ultimately used in decision-making. The background to this argument does include issues of surveillance and the increasing levels of consumer data harvested,[727] however, surveillance is not an issue that heavily features in this report, possibly because users of credit scores (both those watching and those being watched) consider the practice as a financial or commercial necessity rather than an implement of a surveillance society.

The report primarily relies on resources and data found online and a face to face interview. A number of attempts were made to gain access to credit scoring agencies; however these organisations did not wish to contribute to the research. The report progresses by giving an overview of credit scoring, how lenders use data and the legislation governing the system. It then documents two case studies and finally over offers some thoughts on credit scoring's societal impact in the UK.

2. Credit Scoring in the UK

Credit Scoring is a score calculated by 'responsible' lenders to measure the likelihood of loan repayment. Credit scores are derived from statistical and data-mining techniques and are often automated. Credit scoring differs from *credit rating*, because ratings use

[726] BBC, 2012. Paying store cards late can lead to a mortgage refusal http://www.bbc.co.uk/news/business-18832944
ATKINSON, D. The Mail on Sunday (United Kingdom): Scoring a credit own goal Mail on Sunday, The (London, England), May 28, 2006, 2pp
[727] BBC. 2013. Credit reports: Lenders gathering more personal data http://www.bbc.co.uk/news/business-21533587

predictable future information; whereas, credit scoring is primarily concerned with historical information. Nevertheless, lenders are keen to stress that lending decisions are not made solely on credit scores, factors such as, the type of loan sought, the reason for the loan and the likely profitability of the loan are all influential. Equally, factors, such as, the amount of credit already accumulated; late payment history; percentage of total credit in use; holding a mortgage account; the age of the applicant; their employment history; length of time at an address all help to reduce risk levels and effect the success of the application.

Lenders for the most part employ Credit Reference Agencies to provide credit scores; there are 3 main agencies in the UK, Experian, Equifax and CallCredit. Credit Reference Agencies check applicant's information against databases such as, electoral rolls, court records and fraud data – verifying if fraud has been committed by the applicant or if their name has been used by other to do so. (In addition, lenders use anti-fraud agencies; for example, *National Hunter* checks previous applications made by the applicant and verifies if any information differs from the earlier applications). Credit Reference Agencies also search information on addresses and 'linked to' data - records of previous searches made by lenders or organisations in relation to the applicant's name, address and previous addresses. The range and scope of information available to Credit Reference Agencies is increasing, for example, energy suppliers British Gas, BT and Scottish Power now share information on defaults or missed payments with Experian. If requested by an individual, agencies must provide a 'Statutory Credit Report' detailing the information used to calculate a score, there is usually a small fee (£2) for this service.

The sharing of financial information is not exclusive to Credit Reference Agencies and many financial organisations also share, for example, credit card information - HBOS, Barclaycards and MBNA share 'full data', which includes debts, any missed repayments, the amounts normally repaid (if minimum or full payments are made monthly) and any

promotional deals customers may enjoy. It is the culmination of all of these factors which ultimately secures financial loans. In short, Credit Scores present an overview of an applicant's financial past to lenders and this information in turn indicates the probability of these applicants to repay credit.

3. History

The origin of credit scoring and credit checking is decades, if not centuries, old and one widely circulated story in the credit scoring literature tells of its emergence. In a small 19th century American town, a number of shopkeepers who had granted credit to a customer began to converse. The customer in question frequented their stores and had secured credit from all of the shopkeepers. When the shopkeepers realised they had all granted credit to this customer and that his repayments were less than forthcoming the customer's reputation suffered and he failed to receive credit again. The workings of this story are conditional on localized knowledge, where populations are relatively intimate. Within less intimate surroundings credit knowledge can produce complications, especially when personal knowledge and reference points are not as apparent. The move from agrarian to industrial society throughout the 19th and 20th century and the advent of mass produced goods was to play a distinct role in the desire for and use of credit; [728] which in turn provided a catalyst to the development of companies specializing in credit checking.

One of the first companies to specialize in credit checking was Equifax and they based their modus operandi on establishing three c's – character, capacity and capital – in verifying the likelihood of repayment.[729] Equifax began in the US in 1899 and established a large

[728] Williams, B. (2004). Debt for sale: A social history of the credit trap. University of Pennsylvania Press.
[729] BURTON, D., KNIGHTS, D., LEYSHON, A., ALFEROFF, C. and SIGNORETTA, P., 2004. Making a Market: the UK Retail Financial Services Industry and the Rise of the Complex Sub-prime Credit Market Competition and Change. VOL 8(NUMB 1), 3-26
Activerain, 2012. Where Credit Scores came from, what they are, and why we have them". http://activerain.com/blogsview/43734/credit-scores-where-did-they-come-from-what-are-they-

database of information on customers – information included: place of employment, marital status, address or memberships to organisations. The databases were in effect files and paper ledgers which included handwritten and typed entries detailing personal information. Up to the 1930s the service was primarily used by mail order companies seeking assurances about their customers before goods were shipped. Other Equifax customers included large department stores or similar organisations selling consumer goods. Throughout the first half of the 20th century the success of such credit checking lead to increasing pressure on Equifax and other credit checking companies as the management of the databases and the training of staff skilled in making credit judgements intensified. The pressure on accuracy and time in making decisions helped to create of a numerical scoring system.[730] Scores related to the customers likelihood of repayment; the scores are still in use today and provide a three digit score ranging from 100 to 999 – the higher the number the more attractive the customer to the lender. An advantage the scores provided was to reduce prejudice, bias or personal opinion due to for example race, religion, sex, marital status. Toward the second-half of the 20th century computerization then took credit checking to another level. In the 1960s financial organisations began to employ credit scoring agencies to insure their products.[731] Fuelled mostly by the advent and success of the credit card; financial organisations were progressively faced with the task of verifying their customer's capabilities of repayment and the customers current level of debt.

The enabling power of computerization to collect and analyse mass amounts of data however was first questioned in the 1970s. Pressing concerns included the possible detrimental effects on personal security and inequality. Throughout this time, and beyond, writers such as Alan Westin challenged computer technologies and their impacts on privacy; his concerns related to the amount and type of information credit scoring companies held on

[730] MyFico. 2007. The History of Credit. http://ficoforums.myfico.com/t5/Understanding-FICO-Scoring/The-History-of-Credit/td-p/19935
[731] Capon, N. (1982). Credit scoring systems: a critical analysis. *The Journal of Marketing*, 82-91.

clients.[732] Especially questionably was information that did not have any relevance to credit, for example, marriage status. Whereas in the 1980s sexual orientation had a divisive impact on credit scoring due to AIDs and the risks of exposure for certain populations. To some degree such implications prevail, as demonstrated in recent work detailing the impact of zip codes demonstrates.[733] Certainly, pressure to eliminate discriminatory lending practices through equality laws have helped to ease the practice; however computerisation and algorithmic calculations do allow financial organisations to apply questionable practices; for example, setting of parameters and risk factors that may discriminate. [734]

4. Legal provisions (regulation)

Within the UK the main piece of regulation guiding credit scoring is the Consumer Credit Act (1974). The Act requires those businesses dealing with credit to be licenced by the Office of Fair Trading (OFT). Credit companies in the UK cannot operate without the license and there are approximately 120,000 license holders in the UK. If the OFT deems a business to be 'deceitful or oppressive or otherwise unfair or improper' then trading licenses are suspended or revoked. One of the main duties of the OFT is the prevention of 'irresponsible' lending (an emphasis added in the 2006 updated Act).[735] Another legal provision effecting credit scoring has been the Data Protection Act (1988) also has a large influence on credit scoring companies as the information and privacy of individuals must be upheld and data must be stored and used in a responsible manner.[736] Failure to comply has warrants financial penalties. [737]

[732] Westin, A. F., & Baker, M. A. (1974). Databanks in a Free Society: Computers. *Record-Keeping and Privacy'Quadrangle*.
[733] Graham, S. D. (2005). Software-sorted geographies. *Progress in Human Geography*, *29*(5), 562-580.
[734] LEYSHON, A. and THRIFT, N., 2007. The Capitalization of Almost Everything: The Future of Finance and Capitalism Theory, Culture & Society. VOL 24(NUMB 7/8), 97-115
[735] See, www.oft.gov.uk
[736] http://www.legislation.gov.uk/ukpga/1998/29/contents
[737] ibid

5. Scope of application

In the UK credit scoring is a widely used method of risk analysis and it is extremely difficult to gain any sort of financial credit without undergoing some sort of credit check. Indeed, many of the same practices used in credit scoring are also used when customers attempt to open bank accounts, secure a tenancy, buy a mobile phone contract or even when buying forms of insurance. In all instances applicant's details are algormitically checked against databases, such as electoral roles. Indeed, there has been proposals made to link up database such as those held by letting agencies in establishing the credit behaviour of applicants[738] (although this proposal has now been shelved due to issue of data protection). The proliferation and importance of credit scoring as Burton, Knights, et al[739] (2004: p13) suggest, 'In the USA and UK the average adult is credit scored or behaviour scored at least once every week. ….. Although many consumers are unaware of being scored this does not detract from its importance'. In the UK, 7 million credit application were rejected in 2012, of these 1.6 million were loans and 1.2m were credit card applications.[740] All of which emphasizes the importance of a credit score for a sizeable portion of the UK population.

5.1 Practices – what lenders do

The practice of credit scoring, as mentioned, operates to ensure the minimization of risk. In most instances this relates to financial risk and the lending of money. Credit cards are now the most widely used form of credit in the UK.[741] Further expanding the importance of credit, the internet has revolutionized how items are bought and sold. The "internet economy" in

[738] Guardian. 2012. Three easy ways to improve your business's credit rating http://www.guardian.co.uk/small-business-network/2012/jun/11/tart-up-businesses-are-finding-it-increasingly-difficult-to-get-debt-finance-particularly-bank-loa?INTCMP=SRCH

[739] BURTON, D., KNIGHTS, D., LEYSHON, A., ALFEROFF, C. and SIGNORETTA, P., 2004. Making a Market: the UK Retail Financial Services Industry and the Rise of the Complex Sub-prime Credit Market Competition and Change. VOL 8(NUMB 1), 3-26

[740] http://www.debtadvisorycentre.co.uk/advice/nine-million-of-us-avoid-applying-for-things-in-case-we-fail-the-credit-check-0-4079-0.html

[741] http://www.theukcardsassociation.org.uk/Advice_and_links/

2010 was worth £121bn[742] and in 2013 it will account for 11.7% of UK retail sales.[743] An ever expanding range of goods and services available on the internet and these often include commodities bought with credit. [744]

The British Bankers Association state there is a transfer of knowledge between banks and 'Credit reference agencies'.[745] The agreement is of mutual consent; banks provide financial information on individuals to the agencies which helps in the calculation of credit scores and the agencies provide banks with scores based on the amalgamation of information from numerous sources. The agreement is optional, but the benefits are clear. To eradicate issues of data protection, information is only passed with the consent of the customer, banks stipulate to customers when opening an account or applying for credit that the customer's information may be shared in helping the bank to reach consensus on credit suitability. The banks however do limit the information disclosed and it is confined to:

1. a customer has fallen behind with their payments; and
2. the amount owed is not in dispute; and
3. the customer has not made proposals satisfactory to the bank concerning means of repayment following a formal demand; and
4. The customer has been given at least 28 days' notice of the bank's intention to disclose information.
5. Some banks also share performance data about their customers to further support responsible lending. [746]

[742] www.bbc.co.uk/news/business-17405016
[743] http://www.emarketer.com
[744] For further discuss on marketing and control see, Wood, D. M., & Ball, K. (2013). Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism. *Marketing Theory*, *13*(1), 47-67.
[745] http://www.bba.org.uk/customer/article/credit-scoring/borrowing
[746] ibid

Exceptions include, for example, criminal activity when information is disclosed to the police with or without consent.

Customers are placed into narrow categories; categories dictated by, for example, the customer's history of loan repayments, if they were late with repayments, how many loans are held and how much credit they currently are servicing. The questions lenders commonly ask themselves is if customers have received credit and if so what is the likelihood of repayment and making a profit from the loan. Therefore, how a person uses their credit card and the charges incurred on credit are influential in the lenders decision. Credit scoring, as Leyshon and Thrift (1996) attest, is designed to balance the 'information asymmetry'.[747] The asymmetry refers to the fact that there are two conflicting interests in any loan situation, the lender wants to protect their assets (credit) and the customer wants to gain access to assets. Traditionally lenders reviewed a customer's capability to repay through face-to-face interviews or through personal knowledge, such as a bank manager experiences with the person or an examination of the customer's account with the lending organisation. However with the increasing reliance on digitized records in the financial industry personal knowledge is weakened due to the practice of outscoring of information and its collection. Hence, readjustment of the asymmetry increases the importance of systems such as credit scoring. Certainly credit scoring in these terms, provides 'precise and technical calculations on credit risk'[748] and in addition, highlights who may be a 'suitable person to do business with'.[749] These are some of the benefits of credit scoring, indeed what could be added is the speed and clarity for the organisation in estimating the risks. The relevance of the credit scoring

[747] LEYSHON, A. and THRIFT, N., 1996. Financial exclusion and the shifting boundaries of the financial system Environment and Planning A. VOL 28(NUMBER 7), 1150-1156
[748] BURTON, D., KNIGHTS, D., LEYSHON, A., ALFEROFF, C. and SIGNORETTA, P., 2004. Making a Market: the UK Retail Financial Services Industry and the Rise of the Complex Sub-prime Credit Market Competition and Change. VOL 8(NUMB 1), 3-26 (p.5)
[749] LEYSHON, A. and THRIFT, N., 1999. Lists come alive: electronic systems of knowledge and the rise of credit-scoring in retail banking Economy and Society. VOL 28(NUMBER 3), 434-466 (p.440)

has also moved on apace in the UK with the opening-up of financial and credit markets, for instance in the 1990s supermarkets began to expand into the credit market.[750]

5.2 Media coverage

The UK media have given credit scoring considerable coverage in recent years; attention has generally focused on how credit scoring may impact on a customer choice. A plethora of websites offer advice on financial matters, as well as, newspaper supplements, television and radio programmes.[751] Within these formats there is often a clear focus on how to improve you credit score. The emphasis is effectively how to play the system to your advantage.[752] Advice, suggests that if you want to borrow money there is no escaping the credit score, everyone has one and that the first thing a lending organisation will do is check your score. Therefore it is essential that customers come to terms with what their credit score is and how to use it. In what follows I want to present the tips on how to improve a credit score. Most articles I found seemed to go for this style and 10 seems to be the optimum number of tips. Many of the tips are repeated in the articles and here I give a compilation of those I found.

1. Make sure you are on the electoral roll and create a good credit history

The electoral role is one of the first databases that a credit referencing agency will check. The role will confirm identity and place of residence. Also if a person has no credit history

[750]See, http://www.tescobank.com/home/home.html; http://www.sainsburysbank.co.uk/.
[751] See, Fried, Carla (2009) Win at the Credit Scoring Game. *Money.* Sep2009, Vol. 38 Issue 9, p67-70. 4p. Independent. 2012. How to be the perfect customer http://www.independent.co.uk/money/spend-save/how-to-be-the-perfect-customer-8650586.html?origin=internalSearch; Independent. 2013. There's plenty of money to borrow, as long as your record is squeaky clean http://www.independent.co.uk/news/business/comment/james-moore-theres-plenty-of-money-to-borrow-as-long-as-your-record-is-squeaky-clean-8437713.html?origin=internalSearch; http://www.bbc.co.uk/programmes/b006mg74/features/credit-reference-agency.
[752] See, Guardian. 2013. 24 personal finance facts you should know – but probably don't http://www.guardian.co.uk/money/2013/may/28/24-personal-finance-facts?INTCMP=SRCH LEWIS, M. The Daily Telegraph: What's your credit rating? Many of us think we understand credit scoring, but there are plenty of rules to follow:. Daily Telegraph, The (London, England), July 4, 2009, p. 003 5pp

it becomes harder for lenders to predict behaviours and financial activities, without a history or electoral role the chances of rejection are high.

2. Be attentive to debit

As with tip 1, it is essential to maintain a good credit history and this means paying off debits and avoiding missed payments or incurring late charges. Late payment in the previous 12 months are most damaging to credit scores, also cancel unused credit cards, debts and accounts as these can incur charges unknown to the customer.

3. Look at your file and correct mistakes

One of the easiest ways to improve a credit score is to correct mistakes that effect credit applications. Over 30% of applications who have checked have found errors in relation to the information held on them. Mistakes such as the wrong address, misspellings or lines of credit listed as active are in fact redundant – for example an old phone contract. The majority of the tipsters suggest checking a least every year to eradicate errors.

4. What Credit reference agencies don't know – therefore no need to worry about them

It appears there are many misconceptions as to what the agencies use in establishing credit scores. Not included are:

- Parking or driving fines
- Council tax arrears
- Race, religion, colour
- Whether you've checked your file - While this information is held, and appears when you check your file, it isn't passed on to lenders and doesn't play any role in any assessment of you.
- 'Soft searches' - Some lenders will do a soft search on your credit file, to tell you both whether you qualify to borrow from them, and what rate they are

willing to give you. This isn't passed on to other lenders when they credit-check you.

- Salary
- Savings accounts - As savings are not a credit product, they don't appear on credit files. This data is available to banks you hold savings accounts with.
- Medical history
- Criminal record.
- Child Support Agency
- Information on relatives
- Student loans
- Declined applications - Lenders can only see whether you've applied for credit elsewhere, not whether you've been accepted or declined. However, they may be able to guess by examining the credit accounts you have opened.
- Some defaults or missed payments - these stay on file for six years. Bankruptcy is wiped six years from the date you're declared bankrupt, provided it's been discharged.[753]

5. Avoid the rejection spiral

If rejected, check the reason for rejection before reapply elsewhere. Rejection can be caused due to errors and therefore submitting the same application elsewhere is likely to have the same result. In addition, if a number of applications are made and rejected this will have an adverse bearing on future applications.

[753] www.Moneysavingexpert.com

6. Be consistent on applications

Most credit reference agencies use fraud checking systems which can highlight discrepancies in applications. Therefore being consistent is critical, for example, different job titles, mobile phone numbers or other variations may trigger the system. Equally, stability is encouraged by lenders and using a landline phone number, having long-term employment, have the same bank or living at the same address for a number of years may be beneficial to chances of securing credit.

7. Timing of applications

Having a number of credit searches against a customer's name in a short space of time will affect their credit score. However, if applications are staggered the impact will be lessened. Also if events such as a house move or maternity leave are due to take place it is advisable to make the application before the event.

8. A customer is scored as an individual

This tip suggests it is of no direct benefit to be married to a co-applicant as the applicants will be checked individually and then credit linked – where the other persons file is then accounted. Of course, joint products are sold and whether applicants are flat mates, business partners or married should not have an impact on the score. However, it is recommended that if a couple divorces or separates an applicant should apply to be treated separately.

9. Use a 'quotation search' not a 'credit search'

When making an application it is advisable to complete a 'quotation search' or a 'soft search', and not a 'credit search'. Applying in this fashion means the search is not recorded as a credit search, as it would be in relation to an application and therefore the frequency of these searches is irrelevant.

10. Don't lie on the application

As mentioned in Tip 6 discrepancies will be noted and therefore any lies will likely be highlighted therefore to maximize the potential for success it is crucial to be truthful.

6. Stakeholder position

So what does this all mean in terms of surveillance? Credit scoring is widely used and is widely known to exist by customers. Yet, few would think of it in terms of surveillance per se, instead it is just another system that is necessary to partake in, if a particular product or service is needed. When it does seem to come into direct focus is when things go wrong. When refused a credit product, as 7 million Britain's are per annum have been, then the system is questioned and becomes slightly more problematic for those refused credit. Customers are entitled to review the information held on them; of course, they may not be party to how this information was interpreted or its impact on the decision. Credit scoring also presents a relatively different opportunity for customers to freely manipulate this practice, something that is not always present within other systems of monitoring or surveillance. As mentioned customers can enhance their credit score and advice is freely available. Many of the technics discussed are not available to all customers and not all would be in a position to implement changes, for example due to financial commitments or migration status. Indeed, 'financial super-inclusion' or positive discrimination is also a factor.[754] Therefore, the more a customer proves themselves as reliable and risk adverse the more favourable the credit advantages afforded them. These type of customers often receive additional perks , are 'cross-sold' products and avail of service such as no banking fees on current bank account – all so long as they remain in 'good' credit. Indeed, credit scoring is a form of social sorting par excellence.[755] All of which encourages a lack of retrospection on behalf of customers, particularly good customers. However, it is those 'playing the system'

[754] LEYSHON, A. and THRIFT, N., 1996. Financial exclusion and the shifting boundaries of the financial system Environment and Planning A. VOL 28(NUMBER 7), 1150-1156
[755] Lyon, D. (Ed.). (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Routledge.

and those rejected by the system that may be more aware of the implications of this form of monitoring. Equally, effective monitoring and decision-making is a due process that reputable lender must employ.

7. Case Studies

I want to now discuss two sites of controversy in the UK and findings generated from these examples. Both examples deal with events that impacted on how credit systems are working and the resilience of these systems to complications. In the first instance a refusal of credit generated a citizen to question their refusal and then to pursue a quest to find out what credit scoring is and how they could use it to their advantage. The second is an example of an organisation that uses credit scoring to validate its customer – as well as other means. However controversies surround their methods of validation and indeed the high levels of interest they charge when customers default on repayment. Controversies centre on the poor regulation of the industry and how organisations tend to exploit those less advantaged and those in financial need. The pay-day loan organisations are now fighting back against this controversy in order to preserve their place in the market. I begin with playing the system.

7.1 Playing the System

This example relates to the *watched* and in take form an interview with a person has in the past manipulated their credit score to gain favourable rates, position and offers. The interviewee's transitory history may have had some initial influence on the difficulty he encountered; he was born in Eastern Europe and grew up in North America, however for the past 10 years he has lived and worked in the UK. He has a mortgage in the UK, a number of bank accounts and a number of credit cards. In this section I want to highlight a number of

his responses and discuss what I call the *rupture* (as he discovered the problem)*, resilience* (he had in overcoming it) and *status quo* (that result after the incident) that followed.

7.1.1 Rupture

I begin with how the interviewee first became aware of credit scoring. The instance he speaks of revolves around buying a piece of furniture about 10 years ago when credit was refused. The interviewee knew he had enough money in the bank meet the minimum guarantee levels and so was confused by the refusal. Therefore he began to run through the possibilities of why it may have been refused.

> *That was one of those triggers and I just said, no. I need to actually just… I need to really figure out how the hell this functions. What exactly are the criteria which are being used? Also, I had a vague understanding that I had to look at where exactly they were collecting the information. What are the sources? What are the points where the information is being fed through it? This is where it became a factor. Also, how you can… what can I do in order to create a credit history…*

The trigger mentioned spurred the interviewee to question how the system works and to gain a better understanding of its workings. He had suspected his name (which to a UK audience is unusual) was problematic, particularly as it was commonly misspelled and there various accounts, for instance, for gas or electricity did not match his bank account. Also the dispute with a phone company he also suspected was to have a knock-on effect on his credit score. All of which encouraged him to seek out further information

> *The first thing which really started becoming really problematic was because I had a dispute with 3G the telephones. Very crappy service and… I turned them down and I cancelled my contracts verbally over the phone, but then what happened was… that wasn't respected. I didn't pay the bill, but then as a result I was penalised in my credit, so that was one aspect. So, eventually that dispute was resolved, but that really triggered*

me, even when you're in the right to complain and not to pay for something which you clearly did not ask for. How that can be used as an enemy… not an enemy but a kind of detrimental tool against you… so, I just said, this is ridiculous. … there was [also] some kind of a mess-up on how my name or how our name was spelled in Manchester. Then, one of the credit agencies that was used was not picking that up.

This instance was tantamount to raising the interviewee's awareness of credit scoring. It was as far as he can remember the first time he had been refused credit and as far as he was concerned the refusal was unjustified. He elaborates on his awareness at the time

I think I would say that I was aware of it. I was a little bit apprehensive about using it and hence – because of that – it was to my disadvantage personally because of our complex last name and name. There are frequently problems in how it gets actually reported. So, what happens is… for instance, one of the elements which is used for credit scoring here is being registered on the voter's register and I was. One of the credit scoring agencies was not using that. So, what happened is… I couldn't figure out why it is that my credit scoring wasn't giving me the kind of… for some reason I got turned down on one or two occasions for credit despite the fact that when I was offered a credit card, what I was asking was well within the realm of my ability to pay.

Highlighted in the comments are common problems faced when securing credit; errors in the system or contracts being cancelled. These as we have seen have consequences and present tensions and ruptures in how the system worked for the interviewee.

7.1.2 Resilience

While apprehension features in the interviewee's previous comments and may have been something that initially restricted his awareness, the problems resulting from in-corrected information impacted on his access to credit. All of which encouraged him to find out what he had to do to improve his situation. He began by accessing information available online.

I just Googled the stuff. I forget what specifically was there, but generally speaking if you go in any of those compare online sites, they usually have a bit of an indicator of what is being taken into consideration. So, voter's register, previous credit history, and the other thing which I stopped doing is applying for credit. So, if I get any offers – we'll give you a credit card – I don't do it. I go strictly to people with whom I already have a credit history and really interrogate them and convince them based on the kind of stuff that we have. So, it was a really pragmatic combination of what I read online with face-to-face.

As result one of the first actions taken by the interviewee was to correct the spelling of his name and to stop applying for credit. He also registered on the electoral role, was careful with his credit card and his maximum and minimum levels of repayment - which effect credit scores. The interviewee never approached the credit agencies, even though because of other aspects of his life he had submitted FOI requests. The reason he stated was he felt he would get a better response if he talked in person with his bank. Indeed, what may also have been a feature is that the interviewee wanted to play two banks against each other in order to gain a better rate – therefore going to credit agencies may not have affected this financial motive. This was why he initially approached the bank to source what was causing the problems with his credit and he then used their systems of criteria to his advantage:

I think I've been effective in using the particular financial instruments and two bodies – [bank 1 and bank 2] – to our advantage to the point where it actually has gone in our favour and that's a bit of a catch-22 scenario. Once you start putting in positive dynamics by increasing your credit rating, the more you can get. The more you prove that you can with a few small steps, the more you're going to be able to spin it out. So, what I was really apprehensive, seeing the signs of actually… what happens is… if you don't actively engage with this, then you can get a completely warped perspective on what it is that you're capable of. So, usually lucky enough and – I think – smart enough to observe and apply, but lucky enough that you're going to be able to engage people who genuinely listen to you. Then, what happens is… you

can play with the system. You can play to advantage. Facebook. So, let me use that as a metaphor. I think we all – to a certain degree – paint a certain image of ourselves that we're comfortable with and that we want to portray. It's a certain alter-ego. Well, I want to have for the credit scoring agencies and financial institutions is an alter-ego which allows me to have more freedom and more choice. I don't really give a shit what they think about me. I give a shit about how I can influence their decision making so we have more freedom.

As he suggests he learned how they system worked and how best to then use the system. This pattern of credit behaviour has continue to today, as the anger in his statement below indicates,

I was really pissed off about one aspect. Just about two months ago… so, I'm just starting a new job. They reduced by 15% my overdraft limit and they sent me a letter and the reason for it was because I wasn't using it. I said, what the fuck is that? I thought this is about building the credit history and showing that you're responsibly using it. I just said, look, the fact of the matter is that I'm earning more than ever.

An element that may underscore the interviewees appreciations are his justification and acceptance of credit scoring as a necessary tool and a tool that has substantial benefits. His thoughts, due to his personal background, are flavoured by his cynicism of certain infrastructures. The interviewee's parents struggled in a capitalist environment after fleeing a communist regime in the 1980s. As the interviewee admits it gave him a good perspective on both sides of this argument; this is a free market and part of the system is positioning yourself favourably in order to cut the best deal.

7.1.3 Status Quo

The interviewee believes there is an element of control in how a customer can maintain and improve their financial capabilities and credit scoring is one example of how this can be achieved.

> *For me it's the tool that allows me in my life to increase my ability to raise finances, expand my ability to use various lines of credit… generally speaking it gives me a hell of a lot more flexibility. By the way, I just had my credit increased today. So, it's a subject close to my heart and increasingly has become a tool in itself to use as an advantage to me. So, I became almost anally compulsive about what exactly I can use in our favour just so we can have more flexibility and this process has started about seven or eight years ago roughly when I started working at the university where I started getting into the fine detail.*

Nevertheless, the interviewee's thoughts are also balanced with scepticism of how his information is being processed and analysed. As he states,

> *It is definitely a form of surveillance. It's definitely a form of monitoring. I have no means to avoid it, so I needed to find a means to control it or not necessarily control it so much as to massively influence it in passive and active ways….. We don't want to really have a car. We're living in a place where we don't need one, but… shit. I want to have the freedom to buy a fucking car. I want to have the freedom to say, I don't have one because it's a choice or I want to be able to go to Australia for a vacation, but I want to make that choice.*

As the interviewee recognises there is a dilemma between proportionality and necessity. One must recognise you will be credit scored when availing of certain products, however there are issues concerning privacy and the intricate details that may feature in how credit scores are complied.

I don't know whether it's proportional. If it's applied carefully and honestly on both parties – because it's a contractual reality – then it can be that. However, if it's applied as an abuse of authority – and it can be like that, too – it can be absolutely detrimental to people's reality. So, this is why it's like… that data double needs to be actively maintained because if you don't do this, then what is going on is that this is not a given. This is an actual reality you need to deal with. On one hand this is like a financial miracle alter-ego, but in practice it really opens up phenomenally the opportunities that you have. So, what I was really paranoid about is that at any point there is no financial downward spiral because the same thing that occurs with positive stuff where it gives an inflated positivity… it also happens in the other direction and to me that spells reduction of freedom, reduction of choice, reduction of status almost, and not status in the sense of… shit, man, I get a really blingy kind of thing, but to me it's more about status in the account of opportunities that you're going to have for yourself or your family.

What the interviewee highlights here is an instance that made him question how he gained credit and how he was evaluated when applying for a financial product. The initial refusal lead to gaining a greater and more in-depth knowledge as to how credit scoring works. This in turn has allowed him to use it to his benefit. However, while gaining 'back' control may have been a motive and as he recognises it is a form of surveillance, the problematic and resilience here I feel is centred on using the system to your advantage and not questioning how they system works.

7.2 The Fight Back

This section focuses on the *watcher* and looks to payday loan companies, such as Wonga, QuickQuid, Mister Lender or Money Shop. The term pay-day loan originates from the idea of

securing a loan until one receives their next pay cheque. In recent times Pay-day organisations have made a concerted effort to become more acceptable and main stream, for the most part this has been done through the media and the sponsorship of events or companies. One incident this year received much media coverage when Wonga's sponsorship of Newcastle United football club caused one of its players to refuses to wear the jersey due to his religious beliefs.[756] He later accepted the company's sponsorship after he was photographed gambling in a Newcastle casino.

In this section I want to consider how one company, Wonga, highlights the new impacts of credit finance on UK society. Wonga was launched in 2007 and is a web-based UK company. Founded by the South African's Errol Damelin and Jonty Hurwitz (Damilen had been an investment banker and Hurwitz an internet technologist[757]), the company was the first to use fully automated decisioning technology.[758] Wonga business model is built around short-term loans of less than £5000 and decisions are made in 6 minutes, money is in the customer's account in 15 minutes. Credit decisions are made using information and data from a number of new and novel sources; for example, Facebook. The prospective customer must agree to join the Wonga Facebook page and in doing so also must give access to their friends list and 'timeline'. Wonga then uses some of this information to establish the credit worthiness of the customer, and also uses the friend information to target potential clients. I want to now give an overview of Wonga, which is probably the most widely recognised payday loan lender in the UK and the *rupture, resilience* and *status quo* that resulted.

[756] http://www.independent.co.uk/sport/football/premier-league/papiss-cisse-will-refuse-to-wear-wonga-sponsored-newcastle-shirt--but-seeks-a-pay-rise-to-stay-at-st-james-park-8652995.html
[757] See, http://www.theguardian.com/megas/errol-damelin; http://www.standard.co.uk/lifestyle/london-life/the-two-main-aspects-of-my-life-are-art-and-big-data-meet-jonty-hurwitz-the-geek-sculptor-who-founded-wonga-8615219.html
[758] http://www.theguardian.com/money/2011/oct/16/wonga-algorithm-lending-debt-data

7.2.1 Rupture

The practice of payday loans has caused huge controversy in the UK, because it is seen to target the financially vulnerable, as well as charging extortionate rates of interests. Traditionally payday loans are purchased by those who do not have accesses to more established means of credit purchase, such as through banks. Often customers have exhausted other opportunities of gaining credit due to historical financial difficulty or being on low incomes or government support. Pay-day loans are a well-established form of lending, however in more recent times the market has grown substantially and as a result is now a rather lucrative business in the UK.[759] A major contribution to the growth is the ease of access now provided by companies online; effectively loans can be secured from the comfort of your home within minutes. In some instances there is no need to speak to an operative to secure the loan as credit checks and authorisation is automated. [760]

UK MPs have been vocal in calling for a cap on the charges allowed, have been instrumental in calling for tighter regulation on the industry and in November 2013 the Business, Innovation and Skills Committee questioned representative from pay-day loan organizations, as well as consumer advice bodies. The session explored issues raised in a 2012 report on UK Debt Management and was intended to inform how further regulatory measures would be implemented in 2014. Indeed, some political commentators have called for this type of loan to be rebranded as 'high-cost short-term credit'.[761] In addition, what has also been highlighted is the hidden implications of taking out a pay-day loan, as the act affects credit scores with some mortgage providers. These consequences it has been argued should be highlighted by the pay-day loan organisations.[762] Moreover, much of the concerns raised by MPs and the public have focused on the light touch regulation that has been adapted by the Office of Fair Trading and indeed, by the Financial Service Authority.

[759] http://www.consumerfocus.org.uk/assets/1/files/2010/02/Keeping-the-plates-spinning.PDF
[760] http://www.charisma-network.net/finance/leaky-data-how-wonga-makes-lending-decisions
[761] http://theconversation.com/politicians-go-wild-in-wongaland-but-there-are-bigger-fish-to-fry-19089
[762] http://www.bbc.co.uk/news/business-24814037

Much of the frustration in this regard emanates for the controls and checks that failed to stop the lending and borrowing by UK banks in the lead-up to the financial crisis of 2007.

7.2.2 Resilience

As a result of the Committee and the publicity generated, as well as mounting public and media pressure the industry is 'fighting back' and has launched a charm offensive of sorts.[763] Included has been a commissioned 30 minute film – the film is a sentimental look at the 'real Wonga stories' of 12 customers. Each story begins with a customer's voiceover stating 'I love to..', the uncomplicated message of the film is Wonga's role in helping customers in their quest for betterment.[764] Accompanying this promotional contrivance, the profile of Niall Wass, the chief executive of Wonga, has also been heightened. Since November 2013 he has appeared on number of high profile news programmes such as BBC Newsnight. On these he has sought to vindicate the processes and motives of his organisation. He has stated, customers are happy with the services provided and that the interest rates Wonga provide are competitive. Typically, he states, Wonga's interest rate of 1% per day and Wonga's lending terms are clearly explained to all customers. One of the leading complaints toward the company is that due to the online and automated nature of the company checks and verifications are easily circumvented. Regular examples include customers fraudulently stating they are in employment. Rarely does it appear these discrepancies picked by the online decisioning technology.[765] In addition, Wonga and other loan companies have been adamant in their claims that they are not 'Loan sharks' (a term used for unlicensed lenders, who often use unscrupulous means to gather repayments from extremely high interest loans). Wonga are unequivocal that they never use threatening behaviour toward their

[763] http://www.bbc.co.uk/news/business-24032952
[764] See http://www.youtube.com/watch?v=9Jc-KV0AgkY
[765] http://www.charisma-network.net/finance/leaky-data-how-wonga-makes-lending-decisions

customers; however some media reports suggest customers do face daily phone calls if payments are late; this has been described as 'harassment' by some customers.[766]

7.2.3 Status Quo

The popularity of pay-day loans (£2.2 billion turnover in 2012) emphases the value of the industry and the success of innovative technologies they apply.[767] Initiatives such as using Facebook data are extending the scope and speed of algorithms used, as well as the impact this has on potential customers. The encroachment of credit scoring techniques into social media does present infringements on privacy, trust and choice – prominent in these concerns are levels of accuracy, as a casual comments or behaviours at a later date could influence a customer's, or their friend's, credit score. However, what is not in doubt here is the demand for pay-day loans, particular as a source of finance for those with limited financial credence. And as the Business, Innovation and Skills Committee state, there is a need for tighter regulation and compliance in the industry. One suggestion includes a call for centralized loan database, this is a 'real-time regulatory database' which is used by some US states (and some might argue in common with the centralised debtors list operated in Hungary).[768] Lenders must log all loans and the repayment of those loans within the database and the regulations of the loans and credit histories of applicants can easily be verified. Undoubtedly ethical and surveillance issues abound with this model, but like most surveillance regimes it allows for ease of compliance and management. A phenomenon if current trends continue will remain prevalent for many UK citizens in the future.[769]

[766] http://www.telegraph.co.uk/finance/personalfinance/borrowing/loans/9808188/Wonga-to-get-tougher-on-bad-debtors.html
[767] http://theconversation.com/payday-lenders-are-out-of-time-in-their-fight-against-credit-cap-19398
[768] see EKINT report
[769]See, http://descrier.co.uk/uk/2013/09/huge-growth-payday-loans-companies-offering-7000-interest/; http://www.consumerfocus.org.uk/news/which-payday-lending-research.

8. Conclusion

I have framed the case studies discussed by considering notions of *rupture, resilience and status quo* in order to give some perspective on the lives of UK citizens and their dealings with credit scoring. I use this method because credit scoring and it surveillance implications are problematic in two main ways. Firstly, credit scoring is an issue that affects all who seek credit; no loan company or financial organisation will sanction a loan without due care and diligence that the person can pay back the loan. As we have witnessed it is only when the loan becomes problematic that attention is paid to how calculations and decisions were made. The experiences of the interviewee quoted may be representative of those who have faced these difficulties. Here, the person has difficulties due to common weaknesses in the system. The shortcomings of the system and what the system fails to provide (i.e. credit) are the problem, not the inequalities, tensions and controversies the system perpetuates. These were triggers to credit problems and consumers who face credit problems also have some anomaly hindering their score. Secondly, Wonga is a new generation of lenders, one based entirely online and one almost exclusively reliant on technological decision-making. Such a phenomenon is in its infancy in the UK and the legislation surrounding this form of financial practice requires up-grading.[770] This is a recurring theme is other areas of research conducted for IRISS and elsewhere, a lack of coherence or understanding between business innovators and technologists and those tasked with regulating them.[771] The example used here highlights the turbulence faced by a new industry and indeed the resilience it is demonstrating.

What remains absent in much of this report is surveillance. While the interviewee did recognise surveillance in credit scoring, for him issues of privacy or trust were not to the fore, instead it was how the system could be manipulated and controlled to his advantage. This may or may not be his resilience to surveillance, or it could just be his resilience modern live

[770] http://theconversation.com/let-them-eat-credit-payday-lending-is-a-sign-of-the-times-19863
[771] For more detail see Interview NGO9 WP 4

and how he chooses to purchase credit. I am left feeling that credit scoring is most certainly a form of surveillance, but I am not sure it is viewed in those terms by UK citizens. Instead, sharing personal knowledge with organisations or indeed, the propaganda presented by Wonga, all serve to highlight the commercial imperative that overrides concerns for privacy, risk or trust. The equilibrium or status quo that arise post-shock and post-reliance I would suggest, and as demand for Wonga products may support, is restored by the necessity for a new 'furniture' or the need for a small loan. Commercial leverage overrides political, ethical and moral concerns. In the UK what may however highlight a more political debate in these terms is the clear lack of transparency in how credit scoring operates, particularly when organisations don't highlight risks associated with a pay-day loan. This behaviour is of course synonymous with surveillance and may in due course become a bigger element of the debate. Equally the workings of the credit scoring system and the companies that conduct and maintain these databases is an area that most certainly needs further consideration.

NEIGHBOURHOOD WATCH

IRISS, WP3: Case Study "Neighbourhood Watch in Austria"

Partners involved: IRKS (Reinhard Kreissl, Alexander Neumann)

Abstract

Neighbourhood Watch Programmes (NWP) in the Anglo-American tradition are rare in Austria. Nonetheless publicly perceived problems, fostering NWP schemes in other countries do exist. The solutions or reactions to perceived problems of crime and disorder though are somewhat different due to the specific cultural and historical background of Austrian society.

Austria still displays cultural elements of the authoritarian monarchic spirit rooted in the old Austro-Hungarian Empire. Austrian police embarked rather late on the process of changing from a military to a professional style and elements of community policing are gradually implemented, though only with limited success given the cultural heritage.

Security in Austrian political culture has always been perceived as the task of the State and hence the idea of an active involvement of citizens has not developed. Citizens were expected to report to the police, should they encounter a suspicious or criminal individual, but never getting actively involved themselves. There is one prominent character in Austrian popular culture who embodies this type of mentality: the concierge (*Hausmeister*), who was controlling the tenants in city dwellings, registering every new tenant and even visitors and acting as an extension of low-key surveillance for the police.

Looking for NWP-type activities in Austria there are some cases qualifying as a form of citizen-based surveillance and control. We identified three different approaches in our case

study. We termed them bottom-up, municipal, and administrative. The main characteristics of each of these types are briefly described below.

The bottom up approach: "*The Pro-neighbour association in Vienna*"

The story of Pro-neighbour begins in a neighbourhood in the south of Vienna (2007) and now the scheme is operating all across the country with about 6,000 registered members (2013). Pro-Neighbour is a grass-root movement, initiated by a retired Viennese citizen after more and more burglaries were committed in his neighbourhood. He started a bottom-up campaign in 2007, approaching neighbours, local police and city council members. Rallying for his cause he managed to establish a core group of activists and receive attention of local media. Today he runs a stable network of activists exchanging information and collecting "intelligence" in a lose cooperation with local police forces. Fostering communication processes amongst the members of Pro-neighbour and the (lose) cooperation with local police forces are the backbone of the initiative.

<u>The watchers:</u>

- A group of citizens organizing their own neighbourhood watch scheme in allotment gardens in the suburbs of Vienna.
- Classic approach along the lines of UK NWP "Quote from one of the main activists: *We've been to the UK for knowledge exchange with other NWPs, it was amazing to see what is already possible there*"
- Heavy use of the Internet. Pro-Neighbour runs a blog where registered users can report incidents that are made public via this website. *"Type: I've heard a noise and saw a white box-type lorry with a Eastern-European number plate parking in front of my house, what shall I do now?"*

- On Facebook users are discussing various incidents. Whilst on Facebook the discussion is rather distinctive, the open accessible and anonymous Internet forum of Pro-neighbour offers a platform to discuss concrete incidents as well as share more general thoughts on crime prevention.
- Furthermore Pro-Neighbour runs a YouTube channel where the initiative documents their appearances on local (Austrian) TV stations. (http://www.youtube.com/user/pronachbar)

    - Sponsoring by the local security equipment shops
    - Networking activities with local crime prevention departments of Vienna police, interestingly there is no formal agreement of cooperation between the Vienna police and Pro-Neighbour. In some districts the police and the scheme work together close in others there is almost no exchange of information or cooperation documented between the police and Pro-Neighbour.
    - Pro-neighbour branches established in other cities in Austria (Salzburg and Klagenfurt).
    - Pro-neighbour was presenting its approach at the final conference of the SELPE (Sharing Experiences in Local Policing in Europe) project funded by the EU fight against crime funding scheme.

<u>The watched:</u>

- Ordinary citizens living in the reach of action of the pro-neighbour association – watch for your neighbour

- "Suspicious individuals" (i.e. persons of non-white complexion, fitting with the cultural stereotypes of villains)
-

Municipal security forces: "*City watch*" in the cities of Linz and Wels

Municipal security forces were established as part of a political campaign (mostly from conservative parties) at the communal level. They are supposed to act as a kind civil order force, mostly focussing on incivilities and disorder problems. From a legal perspective they have no police power and primarily they are supposed to increase perceived security in public space.

The watchers

- 30 Citizens on payroll of city council watching citizens, patrolling in police type uniforms, established in 2010 in Linz, designed after a similar scheme in the city of Wels, established in 2009 and staffed with 11 members.
- Legal framework provided by city ordinance, main task to report and react to disorder, focusing on street people, and juvenile subcultures ("Punks")

The public reaction:

- A group of civil activists in Linz is rallying against the "City watch scheme" in the Internet, publishing a booklet (… how to handle the City Watch in Linz) informing the public about the legal limits of this scheme.
- Accusations of racism, incompetence and illegal actions posted by bloggers on the Internet creating a publicly visible resistance against

surveillance by quasi-police force perceived as illegitimate (activists applying a watch the watcher strategy)

- A survey among residents on perception of security conducted in Wels in 2012 showed mixed results: citizens would prefer police over City watch but do see some positive effects, e.g. members of City Watch are visible in public space as opposed to police officers.

The political dimension:

- The establishment of "City watch Linz" fuelled a controversial debate in the local council, right wing council members, claiming a massive increase of crime and violence in Linz – evidence for this claim is shaky. Single cases are used as evidence to justify the need for this scheme.
- With the establishment of these new municipal security forces a debate about the role of police started in both cities.

Administrative "soft" surveillance: "*Wohnpartner program in Vienna*"

Vienna has a long tradition of public housing starting in the 1920ies. About one third of the population is living in apartment buildings (approx.. 200.000 apartments in 2000 housing complexes) owned and managed by the City of Vienna. "Wohnpartners" are a kind of mobile concierge service with a social worker's attitude catering for the mostly multi-cultural resident population of Vienna's public housing. With regard to surveillance one could see these figures as a kind of second-order vigilantes, trying to activate and convince residents to watch over themselves in a non-aggressive manner, but watching their neighbours nonetheless. One of the main reasons for the establishment of Wohnpartners in 2010 was

the increased cultural mix in the public housing estates with migrants flowing in after the fall of the Iron Curtain in 1989. The self declared objective of this scheme is to focus on three main tasks: conflict management, community outreach, and networking.

The watchers:

- Citizens watching citizens, guided by professionally trained members of Wohnpartner
- Members of Wohnpartner identify hotspots and try to solve conflicts

The watched:

- Residents of public housing estates, with a strong focus on ethnic minorities (who are perceived by the locals as “trouble makers”).

The political dimension

- Wohnpartner is a typical welfarist paternalistic solution growing out of the traditional social-democratic policy style of Vienna
- Wohnpartner staff are integrated into the public administration and part of the department of housing of the City of Vienna

For all three cases we collected the available information (documents from Webpages, blogs booklets, hand-outs), analysed media coverage and conducted interviews with activists in some cases. As it turned out there are a number of overarching themes running through all of the above-described schemes.

Who are the main actors?

The type 1 scheme (pro-neighbour) started as a citizen grass-root activity, without any affiliation to one of the political parties represented in city councils in Austria. The City Watch schemes (type 2) were based on initiatives from local council members from right wing, populist parties. Playing on a toxic mix of fear of crime and xenophobia they launched campaigns against a presumed criminal group of migrants, blaming the police for not going effectively after the perpetrators. The issue was taken up by local media fuelling a heated debate about police incompetence, dangerous ethnic groups and the need to defend the citizens against threats linked to drug trafficking, public drinking, theft, pickpocketing, beggars, and crime in general. Along with the claim to establish City Watch as a form of public order policing there was a move to set up more CCTV in public space and to increase control of migrant populations. Despite available evidence and expert testimony to the contrary city administrations finally gave in to satisfy the populist campaigns for more security in public space. The main driver obviously were right wing parties promoting anti-migration, anti-crime, anti-disorder issues under the umbrella of setting up quasi-police forces. At the same time local media were more than happy to take up these controversial issues ("fear of crime sells"). At the same time police kept low profile in the debate. On the one hand they accepted the claim of rising crime and disorder as problems to be addressed in one way or the other, but due to a lack of manpower and cutbacks in funding they pointed out they could not do more. On the other hand the police is the only institution who has the power of robust intervention, they can perform identity checks, arrest a person, ban individuals from certain areas – members of City Watch have to call the police and have no special powers or rights of intervention. Finally there were the pro-asylum, pro-migration groups voicing their concerns about racist ideologies, rising xenophobia and racist attitudes among the members of the City Watch teams. After initial phases of heated public debate

the City Watch teams were established in the cities of Wels and Linz (and later on in a number of other cities like Graz). Up until now there is no independent evidence as to whether there has been an increase in perceived public security due to the new City Watch. Surveys conducted in Linz and Wels show mixed results so far and the police are reluctant to cooperate with these groups.

Finally the Wohnpartner scheme (type 3) in Vienna was set up after a series of public complaints about daily conflicts in public housing estates. These conflicts were framed in the media as “cultural conflicts” among local residents and tenants from other ethnic backgrounds. Support came here also from right of the centre political parties. The main argument was that “foreigners” take over public housing originally meant to provide living space for the traditional Viennese population. With the establishment of the Wohnpartner scheme the city administration managed to contain this controversy. The debate attracted a number of professional social work organisations, seeing an opportunity to get involved in a new field of intervention. Since the approach chosen by Wohnpartner was not narrowly confined to crime and disorder, they managed to avoid a stigmatising debate about crime and ethnic background. Activities comprise urban gardening, all kinds leisure activities, language courses and private lessons for students with learning problems. Hence Wohnpartner is not a Neighbour Watch scheme strictu sensu although it entails some elements of traditional NWP.

Classical Neighbourhood watch schemes like Pro-Neighbour (P-N) from Vienna are not cooperating closely with law enforcement. They neither were initiated nor are they actively supported by the police as an instrument of community policing like in the UK. In the early days of the P-N initiative there was a more or less informal exchange of data with police limited to a very small area in Vienna. This changed about 9 months after the scheme started to work in the local neighbourhood from where it spread out later on. The police stopped the data exchange (maps from the police locating domestic burglaries on a street

level) referring to data protection law, which legally speaking is not the actual problem, since the data was anonymised and only made available to the P-N activists at the level of street, no individual addresses of registered incidents were passed on to P-N.

Police officials or local politicians see neighbourhood watch schemes, addressing “crime problems” like burglary as increasing feelings of insecurity amongst the general public and therefore these activities receive some scepticism from public officials. Citizens are expected to report to the police, should they encounter a suspicious or criminal individual, but never getting actively involved.

Activists on the other hand claim the police are not protecting the general public properly. P-N activists sometimes like to provoke with statements like “We are ready and prepared to go on patrol in our neighbourhood.” Such statements almost automatically trigger a media response in a country, where security is strictly perceived as the task of the State.

Neighbourhood watch schemes in Austria face the *problem* that crime in public perception is an issue to be solved by the police and not by citizens. Neighbourhood watch shames emerge and outlive in districts or areas with a rather high proportion of houses/apartments that are owned by the residents. In central districts of Vienna or other larger cities where most of the apartments are rented or are part of a block of council flats you hardly find any active members of neighbourhood watch schemes. The few neighbourhood watch schemes in Austria as observed and described in this report have a strong community aspect. Neighbours looking after each other, do the grocery shopping when someone is sick, share their private pools or the saunas, organise barbecue parties for the neighbourhood during summer times and so on. Interestingly, from the approximately 15 members of neighbourhood watch schemes in Austria interviewed for this report, no one was below the age of 40, all them reported that it is very hard for the scheme to get young people or young families involved in their activities.

Who are the key stakeholders in the surveillance practice?

As the employees of the “Wohnpartner” programme would not qualify as citizens watching citizens and the municipal security forces are also *watchers on a payroll* we are now concentrating on the members of Pro-Neighbour and their activities in Austria. Data basis for this report are 15 qualitative interviews conducted from March 2013 to September 2013, observation protocols from visits at “safety and prevention days in shopping malls” and official Pro-Neighbour documents we’ve received from our interviewees like flyers or the schemes magazine.

Cooperation and communication between police and neighbourhood watch schemes depends very strong on local actors. For Pro-neighbour who are operating nationwide one can say, that there are districts where the local police is cooperating more closely with the initiative and other districts where there is almost no cooperation or communication. The Austrian Ministry for Interior has no general policy or guidelines how local police should cooperate with those initiatives. The police has a strict and restrictive policy with regard to crime data. No data are made available beyond the annually published crime statistics. While local initiatives would like to have more information the police does not grant access to such intelligence.

Activists from Pro-Neighbour complain that Police officers do not react properly to crime victims. While from a professional perspective of the police officer an incident like a burglary in a private apartment is a daily routine standard situation, the victim is under severe emotional stress. Most crimes in this domain remain unsolved, i.e. the offender is identified in one out of ten cases reported to the police. Most homeowners or tenants have a special insurance and receive compensation for their material damage. But they feel left alone with their personal grievances. This supports a public image of the police as incompetent (they

do not identify the offenders) and disinterested (they do not care for the victims). There are a number of standard complaints brought forward against police forming the basis for ideas of self-help of the NWP type. Police constantly point to limited resources, cutbacks, reduced personnel and other obstacles. At the same time police officials are reluctant to share intelligence with members outside the law enforcement community. NWP activists regularly complain about a lack of cooperation on the side of the police. This situation can be understood against the cultural and historical background of Austria, where police are not a part of civil society but do represent state power. Cooperation with citizens in crime fight is not part of Austrian law enforcement.

The same critique of substandard police performance also is a central issue in the debates about setting up City Watch teams in Austria. Police are criticized for being "invisible" in public space, for not responding to emergency calls in time and not being able to contain disorder and petty crimes.

"RESILIENCE" OR: What controversies have arisen in the history of that surveillance practice. Who was involved and how was it resolved?[772]

Looking at the activities of NWP in Austria, or more precisely at the few activities that would qualify as a sort of NWP a few observations can be made with regard to resilience. First of all, the fact that a public debate about the pros and cons of such approaches developed can be interpreted as a sign of resilience against the background of authoritarian quietism in Austria. Taking up a problem like crime and disorder as a topic of public debate and not addressing the authorities to solve it, is in itself a resilient reaction, since it can be interpreted as activation of community resources to handle a community problem. Furthermore the emergence of controversial debates, focussing on questions like: how do we – as a community – want to handle a given problem, and what is the nature of the problem in the first place – a crime problem or a problem of social injustice - also could qualify as a form of

[772] Reference to be made to: http://www.irissproject.eu/tiki/tiki-list_file_gallery.php?galleryId=12

resilience, since the community through such controversies develops an understanding of its own identity.

The question of what forms of resilience towards surveillance measures can be identified has to be discussed differently with regard to neighbourhood watch schemes. Citizens are not scrutinized by the state or by companies as in the ANPR or Credit Scoring case studies. Citizens who join neighbourhood watch schemes can become active watchers.

Within the whole case study including Austria, Germany, Scotland (who share lot's of similarities) and Spain basically two forms of resilience can be identified. In Spain you find examples for watching the watchers. There are movements controlling the police controlling migrants at public spaces. The second more common form of resilience in countries like Austria can be described as a group devolving an understanding of its own identity through their controversial debate on how as a community they want to handle a crime problem without addressing the law enforcement units that should traditionally take care of this problem.

How, where and when it has been referred to in the media

Pro-Neighbour is quite actively disseminating its agenda. On their YouTube channel several appearances on regional as well as on nation-wide TV are documented[773]. Basically the question: How effective are neighbourhood watch schemes in addition to traditional police work in Austria always pops up when burglary rates are increasing (before Christmas[774] and during the summer holidays). Every 3-4 months you can find articles in the major

[773] http://www.youtube.com/user/pronachbar
[774] for example from November 2013: http://www.österreich.at/nachrichten/Bis-zu-55-Einbrueche-pro-Tag-in-Oesterreich/123074035

newspapers of this country interviewing the general secretary of the scheme on his perception of the increasing burglary rates. For this report we've analysed the articles from 2013 dealing with Pro-Neighbour and generally speaking one can identify two different strategies that Pro-Neighbour is adapting to this question. Sometimes they tend to give a, for the Austrian debate, provocative answer and announce that their members will start to war uniforms and run patrols on the street level as the police is inefficiently protecting the citizens. In fact the member's Pro-Neighbour are neither uniformed nor they are patrolling their neighbourhood. The second communication strategy that can be identified is, that Pro-Neighbour is emphasising in their media statements that they are wishing and willing to cooperate with the police and that communication is the pest preventive measure one can think off[775].

When, where and how it has been implemented; who led the implementation. Who else was involved in it?

The biggest Austrian neighbourhood watch scheme Pro-neighbour started its activities back in 2007. There is one community safety association registered in a district in Vienna which is active since 2003/04. The initiative is called "Sicherheitspartnerschaft Oberdöbling" which literally can be translated as "Community Safety Association Oberdöbling". This is the oldest active neighbourhood watch scheme in Austria, but with a stronger emphasis on community safety and no ambitions to expand it's activities nation-wide. Oberdöbling is a posh and expensive upper-class district of the city of Vienna. As opposed to Pro-neighbour this "Community Safety Association Oberdöbling" was initiated and is supported by their local police station.

[775] http://www.ots.at/presseaussendung/OTS_20130709_OTS0045/vertreter-der-polizei-aus-valencia-zu-besuch-bei-pronachbar-in-wien-bild

When Pro-Neighbour was launched, back in 2007, they called themselves "Help burglary". A single citizen started this grass-root movement on the street level. Handing out flyers to other citizens in his living area after a series of burglaries happened. The aim of the initiative was initially not to expand across the whole country, the activities of "Help burglary" now Pro-Neighbour was concentrating on the local neighbourhood where it first started. At one of the first meetings of the group the idea came up to host a website where users could obtain information about burglaries and other incidents that occurred in their living area. The story goes that a young computer-scientist was attending the meeting and offering his skills to the group for free it was possible to set-up the first website. From that moment and through the media response, Pro-Neighbour grew bigger and now has approx. 6,000 registered users/members. Not all of them are active "neighbourhood watchers" but all have access to the reports the network provides through its mailing list. Although the website first was focussing on issues in the immediate neighbourhood, the initiative later on developed into a communication platform for its members. Interested citizens can register online and receive information about incidents in the district they are living.

How it is currently regulated

The Security Police Act (Sicherheitspolizeigesetz – öSPG) states that only the Police is entitled to investigate crimes and to pursue suspects and perform stop and search activities. Private security companies or neighbourhood watch schemes are not allowed to stop citizens and to perform identify verifications as the Police can do. Pro-Neighbour is organised as a non-profit association and is not receiving any public funding. The membership is free, although donations and sponsors are welcome. The activities of Pro Neighbour as a non-profit association are regulated by the Austrian Associations Act 2002 (Vereinsgesetz 2002).

Whether the practice is externally accountable, and if so, to whom

Pro-Neighbour is a private non-profit organisation and has no funding or support from any official institution (e.g. the police) there is no mandatory reporting of the results of their activities. Pro-Neighbour provides a lot of information material on crime preventive measures on their website and informs their members on incidents through a mailing-list, their Facebook profile and the website. For registered district coordinators there is an internal area where those members can access statistics, forms and information restricted to co-ordinating members of the scheme. Pro-Neighbour operates under the general legal framework for voluntary charitable associations. There are only few formal and bureaucratic requirements (such as producing an annual report about activities and budget) but no special regulatory regime regarding data protection or privacy issues is applicable for this kind of organisation in Austria.

How the organization or public authority has engaged with the public around its use of the surveillance practice

Pro-Neighbour is regularly present at several national “security related events” like crime prevention days or neighbourhood fairs. 2011 Pro-Neighbour visited the UK and signed a Memorandum of Understanding with a British neighbourhood watch scheme (NHWN - Neighbourhood Watch and Home Watch Network). Since 2009 Pro-Neighbour is listed in the EUCPN (European Crime Prevention Network) as a good practice example[776] for crime prevention and Pro-Neighbour was awarded in 2012 with the European Crime Prevention Award. In 2013 the SELPE Project (Sharing Experiences in Local Policing in Europe) took note of Pro-Neighbour and invited representatives from the Association to several project workshops.

[776] http://www.eucpn.org/goodpractice/showdoc.asp?docid=201

IRISS, WP3: Case Study "Neighbourhood Watch in Germany"

Partners involved: UH (Nils Zurawski), UniBW (Wolfgang Bonß, Daniel Fischer)

Abstract

In Germany the establishment of internal security *("innere Sicherheit")* in general or community safety in particular is and has always been very much and foremost the domain of the police. As a result, *Neighbourhood Watch* schemes, or more broadly, any activities or initiatives concerning public safety that were started or based on civil engagement only, do rarely exist, - and if, they are very heterogenous regarding their purposes and methods. On the other hand it exists a tradition of police triggered and guided active involvement of citizens in the field of crime prevention and the surveillance of suspects. However this is always facing two major limitations:

a) Since political decisions about the structure or actions of the police are made on the level of the federal state (*Bundesland*), this creates a very heterogeneous picture of the cooperation between the police and citizens throughout the country. There is no role model or stereotype organisation that can be found in every town or city but only scattered, very different, mostly periodic forms of civil engagement.

b) There are huge historical resentments against organised private efforts in public security issues. Whenever somebody demands another attempt of establishing community safety by involving citizens to watch each other, there's a classical set of arguments ("right winged vigilants") and vocabulary ("civil patrol", "militia") that is used to dismiss these ideas.

These two aspects – federal organisation of security matters and scepticism against private efforts - characterize the German constellation briefly and should serve as general

background information giving a more detailed description. First we will describe the special history of non governmental security organisations in Germany. We then move on to look at current attempts to activate people to contribute to community safety and similar goals.

0. Ethical Issues

The following analysis is based on material that mainly has been found through desk research (internet sources, media reports both online and print, video and audio material on internet platforms). However, two quotes used in this text are taken from interviews that were done for WP4. These interviews meet the requirements of the ethical standards of IRISS: Before the interview started, people were informed about the idea of IRISS and what the interview material is going to be used for.

1. The history of the surveillance practice as used by a particular organization or public authority (also relating to the questions: "What is the legitimacy of Neighbourhood Watch?" and "Can any relationship be found between crime figures or is there potential to investigate whether NW schemes were established in areas that had perceived high crime?")

1.1 Early Forms of Neighbourhood Watch:

"Bürgerwehr"

Since the foundation of the German national state in 1871, there's a long history of so called "*Bürgerwehr*" organisations, which can be seen as local or regional defence associations against external threats, as well as police-like forces that control internal security. They have

their roots partly in the middle ages and today exist only as cultural, folkloristic clubs.[777] Nevertheless the term “Bürgerwehr” is still used in a slightly negative or at least sceptical way to describe initiatives that resemble neighbourhood watch schemes. A problem of the “Bürgerwehr” in its history is that its functions and competences in regard to the official army or upcoming police institutions could be distinguished less and less precisely within the process of establishing all kinds of governmental institutions that should subsequently take care of security issues. Some “Bürgerwehr”-organisations were simply integrated into the military forces, some continued to exist without exercising any function over years. In the early 20th century, during the political crisis of Weimar, “Bürgerwehr”, like all organisations with reference to surveillance or control effects or with some military potential were targeted and instrumentalised by the competing political forces. These aspects make up the ambivalent character of the term “Bürgerwehr”: On the one hand its cultural elements, directed at preserving traditional ways of life, which can be observed in all currently existing “Bürgerwehr”-organisations (this in turn shows its proximity to a conservative, middle-class milieu); on the other hand its police-like, executional element with unclear functions, competences and responsibilities.

The “Blockwart”-Years

During the NS-regime Germany has witnessed its probably most prominent and extreme form of a neighbourhood watch institution: The “Blockwart”, the lowest position within the NS-Organisation was the headmaster of apartment buildings in towns and cities. As such, he had the most direct contact with the population on a daily basis. He reported all activities and encounters of the house residents to his disciplinarian, who again collected information from different “Blocks”. Schmiechen-Ackermann calls the “Blockwart” a constitutional element of the NS Regime, because his physical omnipresence manifested the totalitarian ideology in

[777] As such, these are now subject to historical and cultural research, for example: Ertz, Michael: Geschichte der Bürgerwehr der Stadt Bretten, Bretten, Bürgermeisteramt Bretten, 1994.

people's everyday life.[778] "Little Hitler" was the nickname among the people, because his observations were the basis for so-called "political judgements" that could lead to imprisonment. Historical research discusses at least critically the thesis, that "the Blockwarts contribution to the stability of the NS Regime was even higher than that of the Gestapo."[779]

A character similar to that of the "Blockwart" figure was also existent in the Stasi-Regime of the GDR: It was required to register every (short- and longterm) visit of non-house residents at the "Hausvertrauensmann" (i.e.: "Trusted House Resident"); especially visitors from outside the GDR had to provide evidence for where they have spent their nights during their stay.[780]

The Post-War-Period: Volunteer Police Service

In post World War II Germany, all security institutions were built up anew, and so was the Bürgerwehr, however disposed of all surveillance and security functions. "Blockwarte" however did no longer exist. Security and public safety have ever since been sovereign functions of the police only. In the 1960ies, first cooperations between citizens and the police were introduced: In Baden-Württemberg, a volunteer police service ("Freiwilliger Polizeidienst") was introduced in 1963 (followed up in Bavaria in 1996, in Saxonia 1998, Hessen 2000). It requires some education offered by the police schools, after which the volunteer police officer cannot be distinguished from a real police officer at first sight, wearing uniforms and weapons. Differences lie in its legal status and the restricted fields of work. Community crime prevention was only added in 1998 to its fields of work in Baden

[778] SCHMIECHEN-ACKERMANN, DETLEF: „DER „BLOCKWART" -Die unteren Parteifunktionäre im nationalsozialistischen Terror- und Überwachungsapparat", in: Vierteljahrshefte für Zeitgeschichte, Vol 48 (4), p 575-602.

[779] Weyrather, Irmgarth: Die braune Fassade, Über d. Zusammenleben von Nazis, Kommunisten, Juden, Sozialdemokraten, Bürgern u. Arb. im Berliner Mietshaus, Literatur und Erfahrung 3 (1982, 10). S. 44.

[780] See III. §14 in: http://www.verfassungen.de/de/ddr/meldeordnung65.htm

Würtemmberg. In Bavaria, Saxonia, Hessen the "volunteer police service" has been introduced with community crime prevention as its dominant purpose, which is reflected by its different denomination as "Sicherheitswacht" (security guards).

An interesting quote which again shows the typically german constellation described in this chapter can be found on the website of the bavarian police[781]:

> *"The Sicherheitswacht is no auxiliary police. It should not replace but complement the work of the police. Also it is no "Bürgerwehr" (i.e. an uncontrolled association of citizens who believe they must take care of law and order themselves. The Sicherheitswacht is the better and constitutional alternative."*[782]

Berlin had volunteer police services even since 1962, in both parts of the city: "Freiwillige Polizeireserve" in West-Berlin, "Betriebskampfgruppe" in East-Berlin. Its main tasks were the protection of buildings. However, after the reunification of Germany, there were some scandals about right extremist people who were active in these volunteer services[783], with the organisations subsequently closed down.[784]

---

[781] In Bavaria, there are currently 118 places where there are Sicherheitswacht-Organisations, with 720 citizens engaged (including 240 women, and 46 people from foreign countries: see: http://www.polizei.bayern.de/wir/sicherheitswacht/index.html/299 Every Sicherheitswacht can be suspended (and refounded again) by the local governments, which leads to ongoing debates every time specific events happen (see point "Media reports").

[782] Original quote, http://www.polizei.bayern.de/wir/sicherheitswacht/index.html/304: "Die Sicherheitswacht ist keine Hilfspolizei. Sie kann und soll die Arbeit der Polizei nicht ersetzen, sondern ergänzen. Sie ist auch keine "Bürgerwehr" (unkontrollierter Zusammenschlüssen von Bürgern, die glauben, selbst für Recht und Ordnung sorgen zu müssen). Die Sicherheitswacht ist die bessere und rechtstaatliche Alternative."

[783] http://www.focus.de/politik/deutschland/polizeiskandal-berliner-hilfssheriffs-in-morde-verwickelt_aid_142629.html

http://www.focus.de/politik/deutschland/polizeiskandal-neonazis-und-ganoven-in-berlin-auf-streife_aid_140345.html

[784] In Baden Württemberg the organisation has also been closed down after the federal elections in 2012, which was won by a non-conservatice government for the first in the history of Baden-

Summed up, all initiatives that are triggered by the government and that are connected to the police are critically discussed:

- Sicherheitswacht would only produce a higher feeling of security, without really making streets more secure (Police)

- Sicherheitswacht is just a way of saving money for the government and to outsource some of the functions the police is supposed to perform (opposition).

- Mostly nationalistic, conservative or even right winged cititizen would apply for a job at the Sicherheitswacht, who are likely to abuse their power (citizens, left wing/liberal activists)

- It is irresponsible to leave the important and sometimes dangerous task of securing the community to low qualified people (police)

- Sicherheitswacht organisations prevent ordinary citizens from being responsible themselves, it constructs a difference of meaning between citizens where there should be none (opinion uttered by a journalist)

Counter arguments are that:

- People would appreciate any way of presence of official actors that stand for law and order (Opinion of a Sicherheitswacht member)

- There are no dangerous situations that would demand for police officers. Sicherheitswacht members are advised to call the police whenever things get complicated (Government/Sicherheitswacht members).

Würtemmberg. The official reason was, that accurate police service cannot be delivered by non professionals which endangers especially the volunteers: http://www.badische-zeitung.de/suedwest-1/freiwilliger-polizeidienst-als-auslaufmodell--67593191.html

1.2 Contemporary Initiatives/Forms of „Neighbourhood Watch“ in Germany today

In this section we would like to introduce some examples of Neighbourhood Watch Schemes, that are not connected to police work directly.

Kiezläufer (Hamburg, Berlin)

Kiezläufer are people that walk around certain inner city areas. Most probably “Kiez” corresponds best to what “neighbourhood” actually indicates: A spatially limited area, producing a sense of belonging with little mobility into/out of the Kiez. Other than the term “urban quarter” or “district” the term Kiez really includes some shared mentality, which in some cases has some infamous elements (a good example is St. Pauli in Hamburg). It is important to note, that Kiez, as a term as well an idea, does exists in cities of northern Germany mainly. Kiez culture may exist to a low extent in Cologne, Frankfurt, but, especially in Berlin and Hamburg. The idea of Kiezläufer came into being in the 2001/2002, especially as a reaction to increasingly brutal violence among young people.[785] As one can see in the evaluation for Hamburg-Veddel, the idea is born out of an institutional arrangement called “Stärken vor Ort” (“Strengthening on site”)[786] funded by the *Bundesministerium für Familie, Senioren, Frauen und Jugend (ministry of families, pensioners, women and youth)*, the European Social Funds and the European Union. The idea did not come from the Kiez-locals, but was introduced by institutions like the Hamburg Police, the Institut für konstruktive Konfliktaustragung und Mediation (IKM) and an organization called “Get the Kick e.V.”. However they used locals as agents, often those that had previous experiences with delinquencies.

[785] See: Veddeler Kiezläufer – Zwischenevaluation – August 2010: http://www.inklusion-sh.eu/uploads/media/Zwischenevaluation_Veddeler_Kiezl%C3%A4ufer_August_2010.pdf
[786] http://www.staerken-vor-ort.de/

Other Kiezläufer-Organisations, such as in Berlin-Moabit, have a broader spectrum of work: Vandalism, violence, trash and bulky waste on sidewalks and in parks are a problem in Moabit-West, which is supposed to be solved by the Kiezläufer, together with the "Quartiersmanagement" and the residents.[787] In Berlin-Wedding the focus on a clean and inviting neighborhood is even the dominating task. Their goal is to establish a sense of responsibility for behaviour in the streets – as the problem is not that people leave their waste on the streets or act violently, but that those people can be quite sure, that nobody will intervene when they do so.[788]

Generally, all Kiezläufer organisations have an institutional structure. Their work method is developed by scientific consultancy (social sciences, psychology), Kiezläufer themselves must pass some education, they have to register and report their work to the police.

Wachsame Nachbarn

The project "Wachsame Nachbarn" (*alert neighbour*), has also been initiated by the police, as a reaction to the increasing numbers of burglary all over Germany in 2004. Since then the initiative is regularly present in the newspapers, especially when statistics about burglary are rising.[789] It's one of a small number of projects, which can be found in the whole country. It's about informing people on security measures against burglary, one of which is the will and courage to have a look at one's neighbour house too, to address people in the streets, that obviously do not come from that area. The project's only goal lies in the establishment of security within an urban quarter, it has no positive idea of a functioning community life within it, but seeks to protect the houses of the residents from external threats. Stickers on postboxes and houses shall act as a deterrent to burglers.

[787] http://www.moabitwest.de/Kiezlaeufer.3177.0.html

[788] http://www.pankstrasse-quartier.de/Kiezlaeufer-fuer-das-Quartier-Reinickendorfer-Pankstrasse.156.0.html

[789] However this wasn't the case in 2013, although burglary statistics showed a massive increase.

On a website, where citizens share their observations, residents can inform themselves about current issues in their neighborhood.[790] To share your observations, you have to register to the site and prove that you're a resident.[791]

Nachtwanderer

Nachtwanderer ("night wanderer") is probably the initiative that is least influenced by the police or other institutions. Following an idea from Sweden from the late 1980ies[792], it has a clear focus on observing people: Parents of youths (15-25) or other residents of similar age are present at places where young people are at night, to prevent conflicts. Most Nachtwanderer organisations can be found in the north of Germany.[793] It's based on voluntary engagement and is directed at obviating troubles among adolescents during the night, while they are in clubs, in public places or in the public transport. Nachtwanderer want to *"improve the social climate by being present, create a decent atmosphere, they want to create a feeling of security, have an appeasing influence and they want to build up trust between them and the young people."* The Nachtwanderer organisations have set up rules to coordinate and control their actions.[794]

The three main aspects of their work from their perspective are:

- to really get in contact with the young people (not just passively observing), but respecting their privacy
- to not solve serious trouble on their own, but call the police instead
- to discuss all incidents within the organisations and protocol these discussion

[790] http://www.weiterstadt.wachsamer-nachbar.de/lastmeldungen.php?loginuser=&loginpasswort=
[791] We are not sure if this already is "Social Media", since the reports of the citizens can be read by the police only, so they are not discussed by other residents online.
[792] http://www.swp.de/metzingen/lokales/metzingen/Nachtwanderer-Die-Idee-entstand-in-Schweden;art5660,1048755
[793] http://www.nachtwanderer.net/ It's interesting that the Nachtwander organisations in the south of Germany are more connected with the police or other official partners, whereas the northern organisations do really act as private initiatives.
[794] http://www.nachtwanderer-huchting.de/fileadmin/dateien/Regeln_fuer_Nachtwanderer.doc

Members of the “Nachtwanderers” are wearing uniforms and logos. There is no regular exchange of information between the single Nachtwanderer organisations, so it really sticks to the neighbourhood level. Once a year however, all Nachtwanderer from Germany have a meeting, where they discuss problems of their work.

“Anwohnerinitiative Bremen” (Residential group, Bremen)

The “Anwohner Initiative” is mentioned here, because of a particular crime prevention measure about 2/3 of their members have taken part in, i.e. SelectaDNA.

SelectaDNA, produced by the company of the same name, is a marker spray with which one can mark movable items, such as jewelry, electronics, computers, furniture or else. The liquid is sprayed on these items. In the case of theft the articles may be traced back to the original owner when found. The unique identifying markers within the liquid (when under UV-light) will show that a given item has been stolen. In addition to marking the items, little stickers on the windows as well as large sized plates at the entrance of the neighbourhood signal that such technology is in use and is aimed at preventing burglaries and theft.

SelectaDNA was chosen by the already existing residential initiative as a means to increase crime prevention, because of earlier incidents of burglaries, albeit in bordering neighbourhoods. This crime prevention measure is but one aspect of this residential initiative, which is far from being a neighhourhood watch scheme.

The initiative is part of German wide league of home owners, which goes back to its origins in 1919. The league is called Verband Wohneigentum e. V. (until: 2005: Deutscher Siedlerbund e. V. - Gesamtverband für Haus- und Wohneigentum). This league is divided in local chapters, some consisting only of a hundred members. Some a few thousands. They are divided along streets and formed around grown neighbourhoods. The membership is voluntary and organized around the notion of neighbourhood, rather than community, the former in a German sense and reading does not have such a strong connotation of control

and inevitability. Its members are interested in a good neighbourhood, in mutual help to a certain degree, stemming from a sense of belonging to the same area and often sharing a common history, either as the first owners of property in then newly developed areas or by living there constantly for a rather long time, 20 or more years. The sense of neighbourhood that our interview partner was referring to may be characterized as that of autonomous home owners, joining forces where necessary, but being very independent in a sense that they do not want to be controlled by others. The initiative is built on a notion of trust and the idea of self-organisation of otherwise independent parties. For example. the local chapter negotiated good oil rates for the annual oil purchase, as roughly 75 houses buying around 100,000 litres of oil (diesel) will get a good price per litre. Also, have they negotiated discounts in local DIY and gardening stores.

In bringing together 70 household for the SelectaDNA scheme, they could negotiate a good price and make sure that plates were erected – also to the benefit of those households not being members of that particular chapter. This was only possible because of an already existing sense of neighbourhood among the members, which can not be induced just like that, as our interview partner claimed.

In a nutshell this initiative has all to do with mutual help among neighbours, with a strong form of self-organisation of people with shared interests, but very little with neighbourhood watch and mutual control – which is most likely present – but which is not the stated, nor the lived purposed of this form of organization. From this it follows that an analysis that wants to compare different forms of organization of neighbourhood or community must take into account its historical roots, its development and its inherent cultures in dealing with mutual help, social control and the autonomy of its members.

Legitimacy of Neighbourhood Watch - summarized theses:

- Long and partly negative tradition of vigilantism and civil security organisations in Germany, based on the experience of NS-Regimes
- Volunteer police services on the land level (with different success, purposes etc.) which are politically contested.
- Private initiatives with a focus more on clean and quite neighbourhoods and good behaviour in the streets; many initiatives just trying to get people together
- Neighbourhood in a way that families, who have lived in a certain area, an area which has a rather homogenous social structure, where people know and share lots of activities with each other cannot be found regularly, especially not in big cities (except for “Kiez”). That’s why neighbourhood has to emerge first, before it can be subject to any “surveillance practice” (lots of research on that)

2. Who are the key stakeholders in the surveillance practice

The Police

In Germany, the police is always involved when it comes to topics related to security measures, to make sure there is strong cooperation among the actors involved. Also the

police always wants to be able to control the amount of activities in that field. The "volunteer police service" is of course a good example for this:

> "The Sicherheitswacht is no auxiliary police. It should not replace but complement the work of the police. Also it is no "Bürgerwehr" (i.e. an uncontrolled association of citizens who believe they must take care of law and order themselves. The Sicherheitswacht is the better and constitutional alternative."[795]

But also the initiative "Wachsame Nachbarn" shows how dominant the police is in the security and surveillance sector: citizens are supposed to inform the police (not the other neighbours) about suspicious behaviour in the neighbourhood, which then decides about actions to be taken.

The government (local level, federal level, european level)

Two strategies can be named as being supportive to the idea of "community":

The policy of "*Quartiersmanagement*", which started in the 1970ies recognizes that social conflicts in modern society (due to poverty, unemployment, immigration, aging society) cannot be solved top-down only, but require on-site development of solutions that involve all kinds of actors: resident citizens, schools, police, city councils, administration. The Bundesministerium für Stadtentwicklung (ministry of urban development) is responsible for this initiative which corresponds to the European Social Funds initiative "*Education,*

[795] Original quote, http://www.polizei.bayern.de/wir/sicherheitswacht/index.html/304: "Die Sicherheitswacht ist keine Hilfspolizei. Sie kann und soll die Arbeit der Polizei nicht ersetzen, sondern ergänzen. Sie ist auch keine "Bürgerwehr" (unkontrollierter Zusammenschlüssen von Bürgern, die glauben, selbst für Recht und Ordnung sorgen zu müssen). Die Sicherheitswacht ist die bessere und rechtstaatliche Alternative."

Economy and Employment in the neighbourhood".[796]

There are many institutions and programs which are born out of these strategies (e.g. "the social city" or an arrangement called "Stärken vor Ort" ("Strengthening on site")[797] funded by the Bundesministerium für Familie, Senioren, Frauen und Jugend, the European Social Funds and the European Union). One very relevant outcome of this policy are local "Neighbourhood Service Centers", where people are encouraged to get in contact with each other, help each other and share mutual interests. So this can be seen as an attempt to create and shape structures that support the (re-) development of social control.[798] Any escalation of conflicts that would demand for increased surveillance, especially with regard to "citizen-to-citizen"- or "self-surveillance" should be avoided. The idea of neigbourhood watch has only once been raised in the political discussion (see 4. Media Reports), but has never been subject to serious planning.

Scientific Actors

The work of the "Kiezläufer" organisations is instructed by scientific consulting by the Institut für konstruktive Konfliktaustragung und Mediation (IKM).

In their plans and reports there's lot of reference to scientific literature..

Private Actors

As shown in the first section of this text, a few initiatives are also formed by citizens in the first place (Nachtwanderer, Anwohnerinitiative Bremen, partly Kiezläufer). However, they look for administrative support and are in contact with the police. These initivatives are few,

---

796 http://www.biwaq.de/cln_032/sid_74B24FCCABCB7BC518645A2C37FF7682/DE/1Programm/node.html?__nnn=true

797 http://www.staerken-vor-ort.de/

798 The decline of „neighbourhood" as social figuration, which deminished the forces of social control is anlalysed by Siebel, Walter (2007): „Ist Nachbarschaft noch möglich?", in Nachbarschaft"; in: Arnold, Daniel (Hg.), München: Callwey Verlag, 2009, p: 7-18.

because they require huge identification: be it with the local area that should be protected and supported (Kiezläufer, Anwohnerinitiative), or with a certain, very specific kind of problem (conflicts among adolescents at night).

All general, "classical" neighbourhood watch schemes – founded by resident citizens, supposed to observe/control/watch over a certain area and to enforce "orderly" behaviour without a specific interest - are being rejected by official institutions (police, councils) as well as by the public in general (see section on media reports).

3. "RESILIENCE" OR: What controversies have arisen in the history of that surveillance practice. Who was involved and how was it resolved?[799]

In Germany, surveillance measures of any kind are always discussed with regard to its totalitarian regimes of the 20th century. Especially the connection between official and non-official surveyors is considered here as the crucial, the genuine "totalitarian" aspect. Without any exaggeration, one could say that this experience of surveillance has been a shock to the system of values and norms of the German society, which can still be traced in a repertoire of interpretative routines, symbols and expressions.

Discussions on introducing "neighbourhood watch schemes" in Germany in the early 1990ies (which were finally rejected), were countered with arguments referring to "Bayern-Stasi", and "informership"/grasses, "…that have its predecessors in the Blockwart."

The police took benefit from these huge ressentiments and solicited its own alternative – "Sicherheitswacht" – with reference to the exact same sentiments:

> *"The Sicherheitswacht is no auxiliary police. It should not replace but complement the work of the police. Also it is no "Bürgerwehr" (i.e. an uncontrolled association of citizens who believe they must take care of law and order themselves. The Sicherheitswacht is the better and constitutional alternative."*

[799] Reference to be made to: http://www.irissproject.eu/tiki/tiki-list_file_gallery.php?galleryId=12

As we've seen in the opening section and analysis, an organized and active way of surveilling the neighbourhood in general can be considered as a "no-go": "Wachsame Nachbarn" is about being watchful of suspicious behaviour by strangers that one can see from one's window, not about patrolling and looking at everybody. Again, the Nachtwanderer organisation is about young people at night, not about having a look at anybody in any place. Thus, to establish some form of "citizen to citizen"-surveillance, one has to specify a certain mutual, one could say "dyadic" relationship between the watchers and the watched (door-to-door neighbours, parents/kids). Only the "Kiezläufer" organisation adresses "people in general". However, these are not randomly recruited amateurs, but "professionals" in a way that they have to pass some education before they are allowed to do their job. They have an institutional context, in which they are monitored themselves.

Some interviews showed that "neighbourhood watch" as a term constitutes a closed discourse, (an insular debate) which has no or rather irrational connections to other beliefs and opinions. I.e., people might be worried about the situation in their neighbourhood, they might hope for "something to happen" and might also be sceptical about the police, but still refuse "neighbourhood watch" as an absurd means to get what they want:

> *Yes that is happening. Here in these houses everybody cares for each other. Even with the changes going on, even when foreigners move in here. But when they are well integrated into the Germans, they take part. Well everybody has its own little spleen. But when there is somebody strange, then he or she will be approached. And someone will notify you: ‚I have seen someone in your garden. Be careful'. And we did not have problems. But you cannot force this. This is grown over years and decades. And this is a problem, too. Try to integrate the new owners or tenants into this structure, that is not easy.* [800]

[800] Original Quote (German Language) Auf die Frage nach Nachbarschaftshilfe:
Ja, das passiert. da muss ich sagen. Hier in den Reihenhäusern, da passt jeder auf den anderen auf. Selbst durch den Tausch bedingt, selbst wenn da Ausländer sind, aber wenn die gut im Deutschen integriert sind, dann machen die mit. Jeder hat seine eigene Macke, das ist klar. Wenn hier einer

Neighouhourhood watch schemes (in an organized manner) or even local CCTV cameras were outright rejected. The interview partner stresses mutual help among neighbours, nothing more. The key to understand this, is the remark about the depth of the relationships that have grown over years and are the basis for such mutual help.

A women from the same estate states this quite distinctively:

> Question on the sign “Alert Neighbour“
>
> *It works with the neighbours. We talk about what is happening, especially with the woman from the one side. She tells me then, ‚there have been strange people here, setting up boxes to collect used clothing. She watches out, she knows when I am not here, and then she just hast a look at it.*
>
> Question on the possibility of neighbourhood watch schemes.
>
> *Some people are nuts. I think that is totally useless. When people live together, and I mean not only sharing estates or houses, but living, nobody has a chance to intrude. That‘s what it‘s all about. It‘s the relationships, that has to work. If that is not working, then you can have someone with a rifle patrolling and it is of no use what so ever. If people have the feeling they have to defend themselves, they have made the step far too late. They have to talk to each other. I think of it from the side of the community (Gemeinschaft)*[801]*.*

läuft der so doof guckt und fremd ist, dann wird der auch schon angesprochen. Da wird auch gesagt: Du ich habe da jemanden bei Dir gesehen - pass mal auf! Und seitdem haben wir auch toi toi toi keine Probleme gehabt. Aber das ist gewachsen. Das können Sie nicht erzwingen. Und das ist das Problem, kriegen sie mal die neuen in diese gewachsene Struktur rein, dass ist gar nicht so einfach. (Int. 5, 21.6.2013, prevention group, WP 4.)

[801] Wachsamer Nachbar / Nachbarschaftshilfe

Nevertheless the gap between individual and institutional responsibilities – once filled by community activities - is mentioned every once in a while. So the “alienation between the work of the police and the citizens” was a key factor in preparing the introduction of the “Sicherheitswacht”; there are also many efforts to establish community life and to address and enforce collective responsibilities.[802]

Only recently (September 2013) there has been a controversy around a very young neighbourhood watch organisation in Würzburg/Bavaria, which probably illustrates once again in a nutshell the German constellation very well: In December 2012 a 23 year old ambulance man founded the “Einsatzgruppe Lupus”, an organisation of about 20 citizens (mostly coming from professions such as ambulance men, firefighters, security agents), that walk and drive around the city of Würzburg, trying to settle disputes among drunken people, to prevent vandalism committed by young people and other. They’re wearing uniforms, with the logo of a wolf (lupus) and a number on the uniforms so that they can be identified in case of controversy.

Das funktioniert mit den Nachbarn. Wir unterhalten uns darüber was passiert, besonders mit der Nachbarin auf der einen Seite, die dann mal sagt, hier sind komische Leute gewesen, die irgendwelche Körbe abgestellt haben für Altkleider z.B. oder so. Sie guckt einfach,wenn Sie weiß, dass ich nicht da bin, dann hat sie einfach ein Auge drauf.

Nachbarschaftswachen

Manche Menschen sind auch bekloppt. Ich finde es völlig überflüssig. Wenn die Menschen miteinander leben, nicht nur wohnen, hat keiner eine Chance einzudringen. Darum geht es. Es ist die Beziehungsebene, die stimmen muss. Wenn das nicht stimmt, kann auch jemand mit dem Gewehr seinen Soldaten machen, dann nützt das dennoch nichts. Wenn Menschen den Eindruck haben, sie müssten sich wehren, haben Sie schon den Schritt viel zu spät gemacht, die müssten viel früher miteinander verständigen. Ich denke da von der Gemeinschaft aus. (Int. 8, 29.7.2013, prevention group, WP 4).

[802] This includes systematical help like in neighbourhood service stations or spontaneous actions: At trains stations passangers are encouraged to „have an eye on each other“ if someone collapses and may fall into the rails.

Moreover they're equipped with various tools like pocket lights, hand-cuffs and capsicum spray (pepper spray). They have a facebook-page[803] where they report about their actions, post pictures of incidents or call for help in finding suspicious people. They also have a youtube-channel,[804] where they show how they work, address or even chase suspects. Furthermore they communicate via an app-based radio-handset "Zello", which records the communication between the members of Einsatzgruppe Lupus and makes them available for the public as podcasts.[805] So they work very transparent and try to be as inclusive as possible. In an incident in early September one of the members made use of the pepper spray, which raised the attention of the media and the police. Since then, the work of Einsatzgruppe Lupus has been debated widely in the local media.[806] Again we can observe, how deeply neighbourhood watch schemes of this kind are refused. The accusation of "being a Bürgerwehr with right-wing tendencies and vigilante justice", "of being secret Blockwarts, that nobody wants" can be read on their facebook page. Also, the police supports this arguments and has asked for a stronger control of this group by the local government: "Since they lack any experience and education to act in such a sensitive fields, which endangers them as well the persons they confront." [807] Another problem is seen by the police, in that the organisation might inspire other people to act on their own. For the moment it has been decided, that they are no longer allowed to wear uniforms or have handcuffs and pepper spray with them.[808] Their patrolling/existence in general can "*currently* not be prohibited on a legal basis", says the police. A closer look at the reactions of the people as reported by the media reveals some other aspects:

- Würzburg is a very safe city which simply doesn't need more efforts to provide security

[803] https://www.facebook.com/einsatzgruppe.lupus
[804] http://www.youtube.com/channel/UC74ByFvipSwbKuMPgK8YjkA/videos
[805] http://zello.com/channels/c/7745239e
[806] see the linklist on http://wuerzburgwiki.de/wiki/Einsatzgruppe_Lupus
[807] http://www.mainpost.de/regional/wuerzburg/lupus_w%FCrzburg_2013.artikel/Stadt-erlaesst-Verbote-gegen-Nachbarschaftswache;art735,7701980
[808] http://www.mainpost.de/regional/wuerzburg/lupus_w%FCrzburg_2013.artikel/Stadt-erlaesst-Verbote-gegen-Nachbarschaftswache;art735,7701980

- People who would engage in that would just try to be important, suffer from “image complex”
- People trust the police very much, and they just don’t want any other organisation in that field.
- The name of the organisation shows way too much reference to NS-related symbols or at least to a military jargon.

4. How, where and when it has been referred to in the media

Reports about domestic „neighbourhood watch schemes“ in the media are never really focussed on a well observed, currently ongoing practice, but analyse with respect to the historical experience of vigilantism in Germany. NWS in Germany, are always a sensitive issue. At best, they report about the latest experiments in that field, like for example the discourse about the “Sicherheitswacht”: In 1992 the idea has been brought up by the federal government, followed by a political discussion which had lots of consent in analysing the problem: rising criminality, lots of burglary, lack of money to pay more police, alienation between police and citizens, lots of anonymity within communities/neighbourhoods. But there was debate about which alternative to vote for: One government party wished to install the volunteer police services (Sicherheitswacht), the other one wanted to establish neighbourhood watches corresponding to the US model. It ended up as “strong state” vs “strong citizen”- discussion.[809] The opposition claimed the situation was much less worrying then it was presented, and all clichés about civil engagement in security issues were presented: There were claims about “Bayern-Stasi”, and “informership”/grasses, “…which has its predecessors among the Blockwart.”[810] The “Sicherheitswacht” was the alternative

[809] The CSU however claimed that strong citizenship like in the US would involve a more liberal weapons law (SZ, 12.11.1992)
[810] Süddeutsche Zeitung, 09.09.1992, S.4.

that was finally voted for; since then, the idea gets introduced during election campaigns (see SZ 19.10.1996 on the land level) or every time a local council has decided to apply for having a Sicherheitswacht in town.[811] Then there's a call for applications, with information about which criteria have to be met and how good or bad this idea works in other towns of the area.[812]

So the media discourse about "Neighborhood Watch" can be analysed as a feature of the specific event. After relevant events, e.g. xenophobic hate crimes such as Solingen 1992[813]), 9/11[814] and especially the terrorist attacks in London and Madrid (See SZ, 9.12.2005), but also after single acts of brutal violence among youths (Berlin, Alexanderplatz 2012), there are discussions about appropriate measures of prevention. In these discussions, the typical arguments of the "more-police-vs-more-civil-engagement" debate are repeated (often complemented by calls for more CCTV).

A second line of reports are those incited by specific crimes – such as burglary – that demand "on site-solutions": A report from a NW member in Britain (Zeit, 23.7.1993: "We are all Deputies") shows, how insufficient police activity is and how important additional efforts organised by citizens are. However the demand for neighbourhood watch to prevent burglary is not very successful, since initiatives like "Wachsame Nachbarn" coordinated by the police already fill that vacancy.

[811] In this case it's the second attempt, which tries to profit from some recent violent robberies in the area: http://www.swp.de/ulm/lokales/kreis_neu_ulm/Ehrenamtlich-auf-Streife;art4333,895565

[812] http://www.swp.de/ulm/lokales/kreis_neu_ulm/Ausbaubares-Erfolgsmodell;art4333,895267. In this case the Sicherheitswacht could not be established because the local polictical parties voted against it. http://www.augsburger-allgemeine.de/illertissen/Buergerpatrouille-ist-abgelehnt-id15251141.html

[813] In Solingen (1993), there was a fatal attack on a house with Turkish residents, which led to discussions about civil engagement: http://soli-komitee-wuppertal.mobi/2013/05/nachtliche-burger-patrouille/

[814] See SZ, 05.08.2002: Vereinigte Staatssicherheit

Then there is a third line of discourse: Calls for active, responsible citizens/neighbourhood watch due to a perception of disorder, of unpleasant situations related to incivilities in one's neighbourhood. There's one report from Neighbourhood Watch members, one living in the US (Zeit, 3.11.1989) that draws the picture of an almost heroic citizen, who reclaims the streets of his hometown from the drug dealers at night, together with his neighbours. Furthermore, the person reports of how positive his relationship with his neighbours has developed, since they found out that they had problems they shared and joined their efforts to face them.[815] In smaller dimensions, something similar can be observed in a town in Schwaben: There's an initiative among neighbours, reporting about smashed bottles, condoms and jabs on playgrounds, that where indicating nighttime excesses. As the police would not do anything against it, they wanted to monitor those places at night, because "under surveillance, they would not behave that way".[816] In the end, the initiative has not got the necessary permission and people are advised to cooperate more strongly with the police. Acting without the police is generally considered to be dangerous, it could even worsen the situation or is uneffective in an "absurd manner".[817]

One also can find reports about negative consequences of neighbourhood watches or vigilantism, typically demonstrated in examples from the US: "The shock about 9/11 has led to a security mania even in private life. In the Wild West, people bought guns and they founded vigilante groups. Today they buy CCTV cameras and denunciate suspects within the scope of Neighbourhood watch." (SZ, 24.4.2008). In Littleton for example, there's an increased number of Neighbourhood watch schemes after the Columbine High School massacre

"The massacre left an desire for revenge, a demand for a scapegoat, no matter how little it may be. This has also sharpended the focus on seemingly unusual behaviour within the

[815] The sarcastic title of that essay is "More joy in life by means of crack" (ZEIT, 3.11.1989)
[816] http://www.schwaebische.de/home_artikel,-Streit-ueber-Buerger-Patrouille-_arid,505641.html
[817] http://www.wochenanzeiger.de/article/44042.html

local Neighbourhood watch scheme. And if there is nothing to report on, even the denounciation of kids behaviours is appreciated." (Zeit, 28.19.1999).[818]

Negative reports reached their climax in 2012, when a young man was shot by a Neighbourhood Watch member in Miami (e.g. SZ, 23.4.2012). This confirmed nearly all prejudices against private or civil efforts in security issues. It is interesting that in the same year, although the crime statistics showed burglary as being the most problematic field in Germany, the option of introducing Neighbourhood Watches has not been mentioned one time in the press all over Germany the days after the were presented.

5. When, where and how it has been implemented; who led the implementation. Who else was involved in it?

Sicherheitswacht

State	Year of implementation (cancelation):
Berlin	1962 (2002)
Baden Württemberg	1963 (2012)
Bavaria	1996
Saxonia	1998
Hessen	2000

Implementation led by the governement, coordinated by the police.

Main tasks:

security services

physical protection (only in case of insufficient police capacities)

patrol duty

traffic supervision

[818] As a result, an 11 year old kid got accused of sexually abusing his younger sister, based on very doubtful observations by the NWS.

supporting the police at big events

In Berlin the Sicherheitswacht was cancelled due to two scandals, in which members of the Sicherheitswacht were involved (including racial discrimination and violent behaviour, the members also had a criminal record). The cancellation in Baden-Württemberg was due to political doubts about the usefulness of a Sicherheitswacht (grade of professionality, need for more education vs. need for more police).

Kiezläufer (Hamburg, Berlin)

The idea of Kiezläufer came into being in the 2001/2002, especially as a reaction to increasingly brutal violence among young people.[819] As one can see in the evaluation for Hamburg-Veddel, the idea is born out of an institutional arrangement called "Stärken vor Ort" ("Strengthening on site")[820] funded by the Bundesministerium für Familie, Senioren, Frauen und Jugend, the European Social Funds and the European Union. The idea did not come from the Kiez-locals, but was introduced by institutions like the Hamburg Police, the Institut für konstruktive Konfliktaustragung und Mediation (IKM) and an organization called "Get the Kick e.V.".However they used locals as agents, often those that had previous experiences with delinquencies.

There are two Kiezläufer-Organisations in Berlin (Moabit, Wedding), also founded in 2002/3. They have a broader spectrum of work: Vandalism, violence, trash and bulky waste on sidewalks and in parks are a problem in Moabit-West. The Kiezläufer, operating as part of the "Quartiersmanagement", consist of residents, often unemployed people are encouraged to take responsibility for their "hood".[821] In Berlin-Wedding the focus on a clean and inviting neighborhood is outspokenly the dominating task. Their goal is to establish a sense of responsibility for behaviour in the streets – as the problem is not that people leave their

[819] See page 5 in Veddeler Kiezläufer – Zwischenevaluation – August 2010: http://www.inklusion-sh.eu/uploads/media/Zwischenevaluation_Veddeler_Kiezl%C3%A4ufer_August_2010.pdf
[820] http://www.staerken-vor-ort.de/
[821] http://www.moabitwest.de/Kiezlaeufer.3177.0.html

waste on the streets or act violently, but that those people can be quite sure, that nobody will intervene when they do so.[822]

Generally, all Kiezläufer organisations have an institutional structure. Their work method is developed and guided by scientific cosultancy (social sciences, psychology).

Wachsamer Nachbar (Alert Neighbour)

The project "Wachsame Nachbarn", also intitiated by the police, as a reaction to the increasing numbers of burglary all over Germany in 2004. Since then the initative is regularly present in the newspapers, especially when statistics about burglary are rising.[823] It's one of a small number of projects, which can be found in the whole country. It's about informing people on security measures against burglary, one of which is the will and courage to have a look at one's neighbor house too, to address people in the streets, that obviously do not come from that area. The project has as its only goal the establishment of security within an urban quarter, it has no positive idea of a functioning community life within it, but seeks to protect the houses of the residents from external threats. Stickers on postboxes and houses should act as a deterrent to burglers.

Residents can inform themselves about current issues in their neighbourhood about a website, where citizens share their observations.[824] To share your observations, you have to register to the site and prove that you're a resident.

There are lots of media reports about succesfull preventions of robberies.[825] The initiative was followed ab by an initiative "K-Einbuch" (No Burglary), which also warns about burglers, but is more focussed on technical devices to protect one's house.

---

[822] http://www.pankstrasse-quartier.de/Kiezlaeufer-fuer-das-Quartier-Reinickendorfer-Pankstrasse.156.0.html

[823] However this wasn't the case in 2013, although burglary statistics showed a massive increase.
[824] http://www.weiterstadt.wachsamer-nachbar.de/lastmeldungen.php?loginuser=&loginpasswort=
[825] http://www.ngz-online.de/rhein-kreis/aktion-wachsamer-nachbar-1.299028
http://www.tagesspiegel.de/berlin/wachsamer-nachbar-entdeckt-einbrecher/7375638.html

Nachtwanderer

Nachtwanderer ("night wanderer") is probably the initative least influenced by the police or other institutions and it also has clear focus on observing people. It's following an idea from Sweden from the late 1980ies[826]: Parents of young people (15-25) or resident people of simlar age as these parents are present at places where young people are at night, to prevent conflicts. Most Nachtwanderer organisations can be found in the north of Germany.[827] It's based on voluntary engagement and is directed at obviating troubles among adolescents during the night while they are in clubs, in public places or in the public transport. Nachtwanderer want to "improve the social climate by being present, create a decent atmosphere, they want to create a feeling of security, have an appeasing influence and they want to build up trust between them and the young people." The Nachtwanderer organisations have set up a set of rules to coordinate and control their actions.[828]

The three main aspects of their work from our perspective are:

- to really get in contact with the young people (not just passively observing), but respecting their privacy
- to not solve serious trouble on their own, but call the police instead
- to discuss all incidents within the organisations and protocol these discussion

Members of the "Nachtwanderers" are wearing uniforms and they have a logo. There is no regular exchange of information between the single Nachtwanderer organisations, so it really sticks to the neighbourhood level. Once a year all Nachtwanderer from Germany have a meeting, where they discuss problems of their work. In 2012 there even was a "international

---

826 http://www.swp.de/metzingen/lokales/metzingen/Nachtwanderer-Die-Idee-entstand-in-Schweden;art5660,1048755

827 http://www.nachtwanderer.net/ It's interesiting that the Nachtwander organisations in the south of Germany are more connected with the police or other official partners, whereas the northern organisations do really act as private initiatives.

828 http://www.nachtwanderer-huchting.de/fileadmin/dateien/Regeln_fuer_Nachtwanderer.doc

Nachtwanderer Treffen" to exchange experiences, discuss problems of their work and how to further promote the idea. [829]

6. How it is currently regulated

Sicherheitswacht:

The regulation is based on federal state law, where there are serveral sub-chapters directed at the status, rights and duties of volunteer police members.

Kiezläufer

There are annual reports about the work of the Kiezläufer.

They are recruited by official institutions (sometimes via employment agencies), applicants have to live on site, do have to pass some training in conflict management and they are paid a minimum salary for their work.

Wachsamer Nachbar

No regulation, just advice and appeals how to help to solve the burglary problem.

Nachtwanderer

There are only internal rules about certain routes and places that have to be observed at what times, rules about how to behave in certain situations (coordinated with the police). Everything is non-official but based on volunteers. No payments. Only internal discussion of incidents.

[829] http://www.lifepr.de/inaktiv/akzent-verlags-gmbh/Grosses-internationales-Nachtwanderer-Treffen-am-See/boxid/306854

7. Whether the practice is externally accountable, and if so, to whom

Sicherheitswacht

Official institution, accountable to the police, the government, the public.

Kiezläufer

Statistics about “number of chats to groups of young people?”, “number of chats to single young people?” “number of forwarding incidents to other institutions” “number of times being called by citizens”, “number of times being called by institutions”, “number of interventions”. These statistics are reported to the government and discussed with the police to decide how to further promote the idea. There are official quality standards that should be met.[830] The statistics are also passed on to the media to report the results to the public.
They report their observations concerning objects (streetlights, waste, all sorts of damgages) to the responsible positions/centers.

Nachtwanderer

Since there is basically no support from sides of any official institutions, there’s also no reporting of results or even statistical monitoring of their work.

8. How the organization or public authority has engaged with the public around its use of the surveillance practice

Sicherheitswacht

Official institution, no specific “marketing”. Some media reports about volunteers and how their experiences are. Since 2005/6, the police in general tries to establish a public

[830] http://www.znf.uni-hamburg.de/Friedensbildung/Friedensbildung14_/KiezlaeuferQualitaetsstandards.pdf

relationship management which also includes information and promotion over the concept of "Sicherheitswacht".

Kiezläufer

The Kiezläufer are surrounded by a variety of events, actors and institutions that are trying to influence community life. There are portraits in a local newspaper[831], interviews with all people who have had contact with the Kiezläufer (other citizens, police officers, children, parents). Every group of Kiezläufer has a website[832] presenting them as friendly, normal people who are familiar with the area they work in.

They have a bureau/station right in the middle of the neighbourhood, where people can come to and ask for help, ask question or report things they have seen.

Wachsame Nachbarn

The police organises many information days, where people can come to and are provided with material (stickers, flyers) to better protect their homes. These events take place regularly at central points within a city/town. There are media reports about these events, including supportive statements by officials (e.g. the mayor, other politicians). Mostly these reports are introduced by a recent burglary (series) that happened close to or even within the town, with quotes from the victims.

Nachtwanderer

Every group of Nachtwanderer has it's own website (none of which offers the possibility of interacting with users there). There are media reports, typically after a new group had been

[831] http://www.saga-gwg.de/opencms/export/sites/default/saga/download_gallery/Unternehmenskommunikation/WIR_5_10_screen.pdf
[832] http://www.moabitwest.de/Diese-Maenner-laufen-fuer-den-Kiez.2197.0.html

founded, explaining the idea of the Nachtwanderers to the public. They have some presence at city festivals and similar events to promote their idea.

IRISS - WP3

Neighbourhood Watch

Spain

Gemma Galdon Clavell[833]

Universitat de Barcelona

Final report, January 1st, 2014

1. Introduction

Spain has had a long history of 'horizontal' surveillance. As a country with a recent authoritarian past, social control and surveillance have been more the norm than the exception. In the 20th Century alone, Spain suffered almost 35 years of military rule (General Primo de Rivera between 1923 and 1930 and Francisco Franco Bahamonde, *El Generalísimo*, between 1939 and 1975), a Civil War (1936-1939) and several episodes of military upheaval in the first years of the Century. In the immediate post-civil war years after 1939, for instance, Francoism had to consolidate its victory in a country where the elections before the *alzamiento* [military uprising] in early 1936 had given the majority to the progressive and revolutionary forces of the Popular Front. In order to do so, those who hadn't died or fled to exile needed to be found and prosecuted. "All criminal activity committed in the national territory during the red domination" had to be brought to the justice

[833] The author would like to thank Cristina Fernández Bessa, an assistant lecturer and colleague at the Universitat de Barcelona, for her research assistance and insight in preparing this report.

of the many special courts set up in order to organize the purging of reds, communists, separatists and freemasons.

In a country where most of the population lived in rural areas[834] and power was organized locally, this task meant establishing local networks of power and control, structured around the institutions controlled by or aligned with the regime -the Church, the unelected City Councils, the Falange[835] and the Guardia Civil. In this period, deviancy was not only political, ideological or criminal, but also *moral*. Local priests, Councillors, Falange members and, later, members of the Guardia Civil, were asked by the Courts to send reports and answer queries for information on the activities of virtually everyone –a task which, with exceptions, most fulfilled enthusiastically. In this daily surveillance, the everyday presence of Catholic liturgy, as well as the special role of the Church in a "National-Catholic" regime, meant that local priests, especially in rural areas, played an essential role. Often times, they were the ones who issued the "certificates of adherence to the national movement" that were necessary for a myriad of daily tasks and which were based on "good behavior" –understood as following of Catholic rituals and principles, mainly. Going to Church, and having gone to Church before 1939, was one of the best defense arguments one could have when faced with an investigation.

The recent history of Spain thus shows a stubborn continuity of surveillance, control, domination and revanchism as a political strategy and social dynamic.[836] Vigilantes and grasses have been promoted and sponsored by the state when trying to consolidate military rule. In the last few years, however, the landscape of surveillance practices has changed and diversified, and while state-sponsored versions of 'vigilantism' persist, 'watching others' to prevent crime is taking new forms and dynamics, and new practices of surveillance emerge which, sometimes, are not only about control but also involve care, resistance and dissent.

---

[834] In 1930, only 10 Spanish cities had more than 100,000 inhabitants (Atlas Histórico de España).
[835] *Falange Española*, or *El Movimiento*, was the social organization of Francoism.
[836] For a general history of this period, see, for instance, Carr, Raymond. 2001. *Modern Spain, 1875-1980*. Oxford: Oxford Paperbacks.

The picture of neighborhood watch in Spain, thus, is complex and, at times, counterintuitive. In the following pages, we will to contextualize the phenomenon and attempt to answer the when, where and why of citizen patrols in Spain. Using information from different sources and interviews –as we have been unsuccessful in identifying any other study or academic paper on the subject in the fields of Social Sciences or Criminology- what follows is a picture of neighborhood watch in Spain in all its diversity and complexity, but also a glimpse into the dynamics of fear and resistance in the surveillance society.

2. Neighborhood watch: the legal basis in Spain

Interestingly, the stubborn persistence of horizontal surveillance in the years of dictatorial rule seems to have given way to a paradoxical situation. While surveillance seems to be more 'normalised' at the social level in Spain than in other EU countries,[837] the Spanish legal system has so far been reluctant to promote or legitimize the existence of citizens organizations dedicated to crime prevention. Neighborhood watch or 'citizen patrols', as they are commonly referred to, have therefore never been legal and the State's monopoly of crime prevention and community safety is unquestioned.

In this sense, the 1978 Spanish Constitution establishes that 'The Security Forces, subordinated to the Government, will have as their mission to protect the free exercise of rights and liberties and to guarantee community safety' (Art. 104). The Organic Law that regulates the Security Forces (LOFCSE 2/86) establishes that it is the State and its institutions, at its different levels, that is responsible for maintaining public security, and underscores that this is an exclusive competence reserved to the state and its institutions. The only exception to this monopoly is found in municipalities where there is no local police. In such cases, the duties of the police will be fulfilled by 'personnel working to guard and

[837] Note the normalisation of the use of the ID in Spain compared to the UK, for instance. See Galdon-Clavell, G. and Ouziel, P. (forthcoming) "Spain's *Documento Nacional de Identidad*. An e-ID for the 21st Century with a controversial past". In Boersma, K. *et al.* (eds.) *The History of Surveillance in Europe and Beyond.* London: Routledge.

surveil goods, services and buildings' such as 'guards, watchmen,[838] officers, bailiffs or similar' (Art. 51.2). This opens the possibility for local authorities to hire citizens or private security officers to work on security matters at the municipal level. Similarly, the State's monopoly over public security cannot stop citizens from guarding their property or reporting crimes to the police. Article 259 of the Criminal Procedure Code established that it is mandatory for individuals to report any crime they may have been witness to to a judge.

Therefore, while neighborhood watch schemes are not regulated in Spain, if their only function is to surveil and alert the police when necessary, they are not forbidden. However, their members cannot be recognized as a public authority and if they used force or tried to hold someone they could be charged with several offences, such as illegal detention (Art. 163.4 of the Penal Code).

As for legitimate defense, Spanish law only considers it as an exception of the penal responsibilities one may have if the following requirements concur –that there is an illegitimate attack, that there is a rational need for the use of the means chosen to stop it or repel it, and the absence of a sufficient provocation on the part of the person defending him or herself.

This lack of regulation and institutional authorization of organized citizen patrols has had several consequences. On the one hand, instances of horizontal surveillance have caused much controversy when they have arisen, due to their allegal nature. On the other, the typology of neighborhood watch in Spain is more diverse than in neighboring countries, precisely due to the inexistence of a 'template' or 'model' that citizens can replicate or associate themselves with.

The way that these controversies have developed and been handled by the different stakeholders involved provide insight into cultural and social context, and can contribute to

[838] The original word is 'vigilante'. While English has borrowed the term from Spanish, in Spanish a 'vigilante' is just someone that watches over something.

understanding how surveillance practices embed themselves in broader social processes. A preliminary exploration into these matters will be explored in the last section of this study.

3. A brief note on methodology and research ethics

The methodology used to research the state-of-the-art of neighbourhood watch schemes in Spain has consisted mainly on desk research and some interviews. In the initial phase, instances of neighbourhood watch-like schemes were explored, using primarily newspaper libraries and search engines. The main keywords used were 'patrullas ciudadanas' and 'patrullas vecinales', which translate as 'citizen/neighbourhood patrols' in English, as they are the terms most commonly used to refer to organised groups of citizens that aim to prevent crime and vandalism by patrolling a specific geographical area. Specifically, we have reviewed and analysed 139 news pieces from the newspaper El País between 1978 and 2013. This has been completed with an analysis of other relevant media at the regional and local level, mainly when following specific stories or cases. In this case, 163 pieces have been reviewed. Specific news pieces are often referred to in the paper, providing links in the footnotes –in all cases, the links were testes on December 30, 2013.

Contrary to the case in most Europe, citizen patrols have never been legal in Spain during periods of democratic rule. Therefore, no official institutions keep track of the existence of such schemes, and many exist under the radar. This meant that the research methodology had to explore less traditional means. The research team sent e-mails to colleagues asking for relevant experiences, and students were asked to contribute examples and encouraged to write short papers on specific cases (it was one student, currently a police officer, who pointed us to the experiences from the 80s). Incidentally, one case was identified via twitter, when a member of a citizen patrol tweeted about a forthcoming gathering. In another case, a 'whatsapp'-based patrol was identified, and we decided to join the group. We revealed our identity and purpose to the convenor of the group, but as far as we know, this has never

been revealed to the rest of the participants and we have never contributed to any of the discussions.

After the cases were identified, some members of citizen patrols were contacted via e-mail and phone to conduct exploratory interviews, and four interviews were conducted in person specifically for this report. In all cases, interviewees were made aware of the objective of the study, none of the conversations were recorded and participants are cited throughout the study using their affiliation and not their name to respect their privacy.

The desk research, student comments and interviews provided the basis for an initial map of the state of the art, both geographical and in terms of trends and characteristics, which has been the basis of the study and its exploratory conclusions.

4. A recent history of neighbourhood watch in Spain

While neighborhood watch schemes have been scarce and sporadic, they have emerged periodically since the end of the dictatorship. While they have changed over time -in form, membership, ways of operating, geographic distribution and motives- most people in Spain know what a citizen patrol or 'patrulla ciudadana' is.

The first instances of self-organized neighborhood watch schemes or 'patrols' in Spain appeared in the press in the late 80s, often times linked to the high levels of insecurity and crime of that time, mostly linked to the heroin epidemic. In the early 90, 150,000 people were addicted to heroin in Spain, and in its worst period, the drug killed 300 people per year.

Widespread drug addiction had a clear impact on community safety and people's perception of insecurity, with addicts consuming in public areas, robbing to buy drugs and suffering overdoses at people's doorsteps. The perceived lack of reaction by the authorities led some citizens to organize autonomously to patrol specific areas. In 1991 there were four 'patrullas' in Barcelona's metropolitan area (Barcelona, El Prat, Badalona and Sant Adrià) that chased drug addicts and dealers to literally beat them up and kick them out of their neighborhoods.

While different kinds of patrols appeared in places as diverse as Sagunto, Palma de Mallorca, Valencia, Alicante, Madrid, Almería, Cartagena, Huelva and Pontevedra, in most places the community response to the problem were peaceful demonstrations and meetings with the authorities. In places like Móstoles, San Blas, Alcorcón, Valencia and El Prat, however, there were reported instances of attempted lynching, with members of the neighborhood watch walking around with 'sticks, chains and umbrellas', stopping busses to kick out the drug users and, in one case, chasing a drug addict up into a building and threatening to throw him off.[839] There were also instances of fascist-like bands joining the neighborhood patrols, which were a combination of poverty, prejudice and racism (most drug dealers were said to be Spanish Roma).

In this period, all authorities spoke out against neighborhood watch schemes, and were convinced that the police was the only body that could face the problem properly and within the limits of the law. In 1992 Spain passed its first Community Safety law, giving the police increased powers and establishing new, harsher fines for drug use in public places. The perception of increased awareness and police efficacy in dealing with drug users and dealers (the first instances of community policing in Spain date from this period), as well as the decreasing rates of heroin consumption meant that by the mid-90s the 'patrullas ciudadanas' seemed to be a thing of the past.

But while in the 80s and 90s the authorities were reluctant to accept parapolice schemes, in 2000 something began to change. A report of Cordoba's district attorney's office back then suggested for the first time that in view of the increase in crimes against property, some measures of 'social defense' such as carrying weapons, installing alarms in one's house or organizing neighborhood watches were to be encouraged.[840] The district attorney denied that his office would be in favor of such measures and blamed the debate on some passages of the report being badly written, and the Mayor, the Police and civil society

[839] Interview with a resident, currently a police officer.
[840] 'La fiscalía de Córdoba sugiere a los vecinos que se armen y patrullen', El País, May 16, 2002. Available at http://elpais.com/diario/2002/05/16/espana/1021500017_850215.html

rejected the possibility. Something similar happened in Barcelona when neighborhood patrols reappeared in the city centre during the Spring of 2000. These new patrols did not mobilize against drug users of property crimes, but against the general feeling of insecurity, which they blamed on prostitutes and migrants.[841] The Police and civil society organizations intervened quickly, and several meetings were called to increase the police presence in certain areas and discredit the vigilantes.

However, informal contacts were also made between the citizens patrols and members of the Town Hall, who were flirting with the idea of giving watch members some sort of official recognition of authority so as to make them part of a public-private partnership against insecurity and crime. These efforts were never publicly acknowledged, however, and, as members of the Mayor's office admitted years later, it quickly became obvious that the members of the citizens' patrols were not the best people to give authority to, as they tended to be violent and have problems in dealing with others –and the authorities themselves.[842]

This problem –the problematic 'personality' of neighborhood watch members- was also mentioned in a more recent case, in the context of rural neighborhood watch or 'somatens'.[843] During the medieval ages in certain areas of Spain there was a parapolice and paramilitary corps called 'somatén', which by the 19th Century was mainly operating in rural areas and active in the repression of anarchist and progressive forces. Formally dissolved in 1978,[844] and so far never legal under democratic rule, it reappeared in 1996 as a civil organization, but it only became active in 1999 when an initial group of three men registered as 'somaténs' in a small village near Tarragona and soon after volunteered in a case of serious floods in the area. This led to them being formally recognized by the local authorities and receiving funding and a meeting space. While this is the only active formal 'somatén', rural patrols have recently proliferated in specific areas (Tarragona and Lleida)

[841] 'Las patrullas se quedan solas', El País, August 29, 2000. Available at http://elpais.com/diario/2000/08/29/catalunya/967511248_850215.html
[842] Interview with Barcelona's Councilor for Community Safety at the time. April 2010.
[843] Interview with the Superintendent of the West Police Region (Lleida). December 2013.
[844] 'Recogida de armas a los somatenes', El País, Oct 1, 1978. Avaliable at: http://elpais.com/diario/1978/10/01/espana/276044416_850215.html

due, mainly, to an increase in copper and diesel oil theft in rural areas where the owners of land and farms live away from their property.

According to the media, there are a handful of active rural patrols, and until late 2012 the regional government was playing with the idea of legalizing their activity as a civil aide to regular police. An internal change of government seems to have stopped those intentions, but the 'somaténs' continue to exist and were responsible, in May 2012, of the heart attack suffered by a man who was being chased by a group of them.[845] While the death was deemed accidental, there is something to be said about the situation created by a group of armed men chasing someone they think is a thief, and the levels of stress this can cause on the victim, who is unsure as to what happens when arrested by vigilantes. Also, this case highlights the fact that while rural patrols should always and only alert the police in case of suspicious activity, and never engage in chasing or arresting, this is not always the case.

As mentioned above, the fact that such schemes have never been legal has meant that the landscape of neighborhood watch in Spain is significantly different to that in other European countries. Not only because it is not a generalized or institutionalized phenomenon, but also because when it has arisen, it has done so in very different ways. The absence of a 'template' or 'model' that citizens can replicate has resulted in citizen patrols taking unexpected forms, and neighbors organizing against crime, but also against the police and even against other neighborhood watch schemes.

For the sake of clarity, in the next section we will present the case of 'traditional' patrols – those that we feel can resonate with the European experience. After an initial appraisal of such initiatives and some preliminary analysis and conclusions, the diversity of schemes will be addressed, covering not only the patrols against the police and against neighborhood watch, but also the case of UK-influenced 'online' neighborhood watch.

[845] 'Los Mossos investigan la muerte de un ladrón cuando huía de un somatén en Maials' El Periódico de Catalunya, May 26, 2012. Available at http://www.elperiodico.com/es/noticias/sociedad/los-mossos-investigan-muerte-ladron-cuando-huia-somaten-maials-1839221

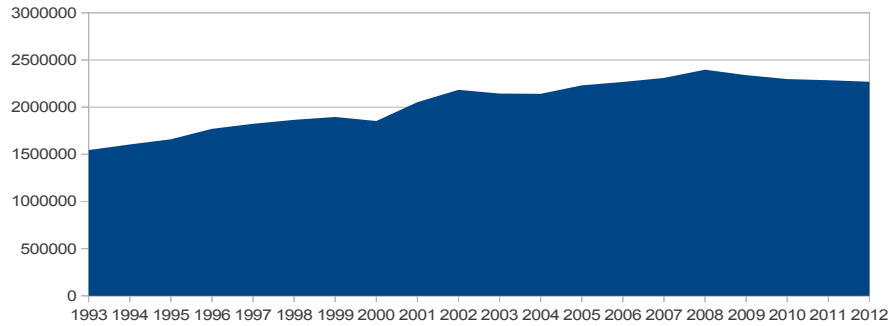
5. A closer look at 'traditional' neighborhood watch in Spain

5.1 Crime and neighborhood watch

According to Díez Ripollés,[846] the characteristics of crime in Spain are: a low level of crime in comparison to other countries of the European Union; the prevalence among the criminal acts of crime against heritage, particularly robberies and thefts; a low rate of crime against persons; and an abuse of imprisonment –for instance, 75% of inmates serve sentences for offences against property or in connection to drugs. These trends have remained constant over the years. According to the official data, since 1998 crimes have remained constant, the fluctuations have been barely perceptible and total figures 'not only have not increased, but you can even see a slight decline'.[847] However, if we try to analyze the evolution of crime in Spain in a rigorous way, we will be faced with a particularly difficult task, especially for independent researchers. In addition to the few police statistics that reflect the real evolution of crime (unreported crime, legislative changes, criminal policy, etc.), statistics published by the Ministry of the Interior of Spain and the police forces are "incomplete, too general and have serious reliability problems.".[848] Additionally, 'in Spain the availability of national victimization surveys has always been very limited, since no official organization has so far assumed the task of conducting them in a systematical manner'.[849] Since 1993, Eurostat has been publishing data for 'known offences' in Spain other EU countries.

Known offences (Spain 1993-2012)

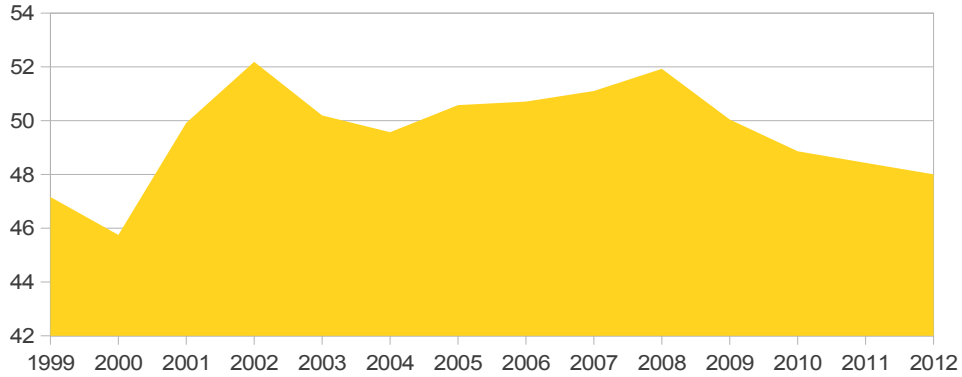
[846] DÍEZ RIPOLLÉS, J.L. (2006) "Algunos rasgos de la delincuencia en España a comienzos del siglo XXI", *Revista Española de Investigación Criminológica*, Núm. 4.
[847] SERRANO GÓMEZ, A., et al. (2006). Evolución de la delincuencia en España según las estadísticas oficiales (1998-2005). Revista de derecho penal y criminología, 2a época, 18. Pg. 577.
[848] AEBI, M. & LINDE, A. (2010). "El misterioso caso de la desaparición de las estadísiticas policiales españolas." *Revista electrónica de Ciencia Penal y Criminología*. http://criminet.ugr.es/recpc/12/recpc12-07.pdf
[849] GARCÍA ESPAÑA E. et al (2010) "Evolución de la delincuencia en España: Análisis longitudinal con encuestas de victimización", Revista Española de Investigación Criminológica Artículo 2, Num. 8.



Source: Own compilation based on data provided by Eurostat and the 2012 yearbook of the Ministry of the Interior

Between 1993 and 2012, the graph shows a steady increase in known offences, with some peaks registered during 2002 and 2008 and slight declines in 1999, 2003, 2004 and 2008. In this period, Spain's population grew from 40.202.260 inhabitants to 47.265.321, so crime figures should be presented in relation to the population, to see if the increase and decrease of known crime´s has been significant or if it is simply due to population increase.

Criminal Rate x 1000 inhabitants (Spain 1992-2012)

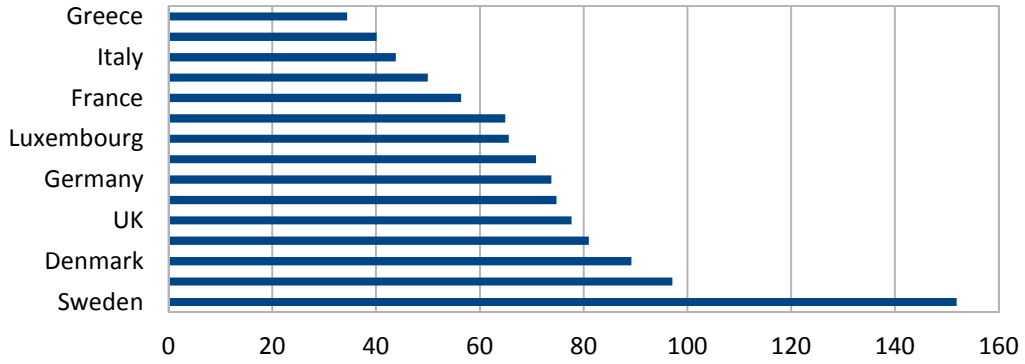


Source: own compilation based on data provided by Eurostat and the 2012 yearbook of the Ministry of The Interior and data from the National Institute of Statistics

In this second graph we can clearly see a pronounced increase of registered criminality between 2000 and 2002. This can be interpreted in different ways: '(...) oscillations or fluctuations observed in the crime trends of the period in review (1998-2005) are mostly due to structural or cyclical factors such as legislative reforms, changes in attitudes and patterns of citizens' complaints or by stronger measures taken by the police in the prosecution of certain crimes, rather than a real increase in criminality'.[850]

On the other hand, we can also see a sustained increase of the criminality rate of from 2004 until 2008, when it sharply decreases. Overall, however, Spain continues to be one of the countries in the European Union with a relatively low crime rate, significantly lower than other large countries such as Germany or The United Kingdom.

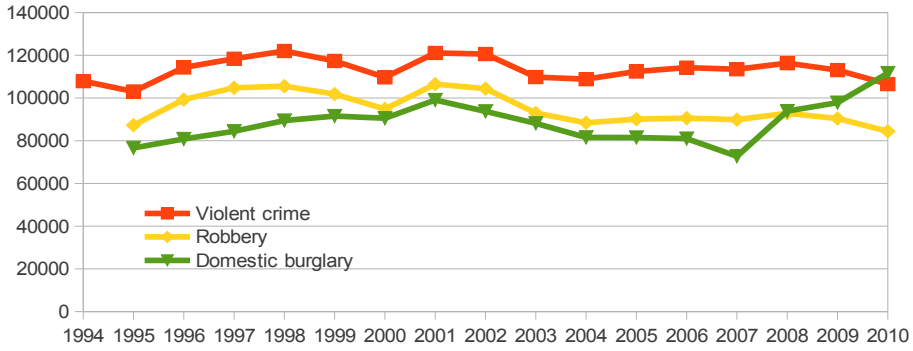
Crime rates (2009)



Source: Eurostat 2009

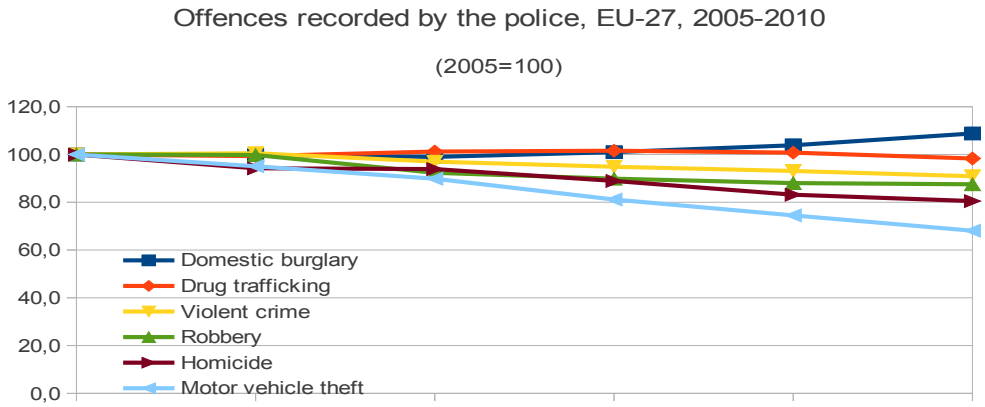
Regarding crime categories, Spain in below the EU average in violent crime and crimes against the person. Property crime, however, is the high and growing.

[850] SERRANO GÓMEZ, A., et al.. (2006). Evolución de la delincuencia en España según las estadísticas oficiales (1998-2005). *Revista de derecho penal y criminología*, 2a época, 18. Pgs. 571-591.



Source: own elaboration using Eurostat

This trend is also observed in the rest of Europe, where, as shown in the following graphic, decrease in robberies and violent crimes is contemporary to the increase of burglaries in residential homes.



Source: Eurostat Yearbook, 2013

Despite the mentioned lack of information of crime statistics in Spain, this brief presentation allows us to size up crime evolution during the last 20 years and assert that crime in Spain has remained low at all times with a slight increase between 2000 and 2002 and another one, also very slight, between 2004 and 2008. However, the low crime rates has not impended concerns due to insecurity and the proliferation of punitivism, nor decreased Spain's incarceration rates.

Despite the displayed figures, the prominence of insecurity in the media and its partisan use have been a constant in Spanish society. As we shall see, the result of this has been a demand for increased security from certain sectors of the population, which sometimes has led to the creation of neighborhood watch schemes.

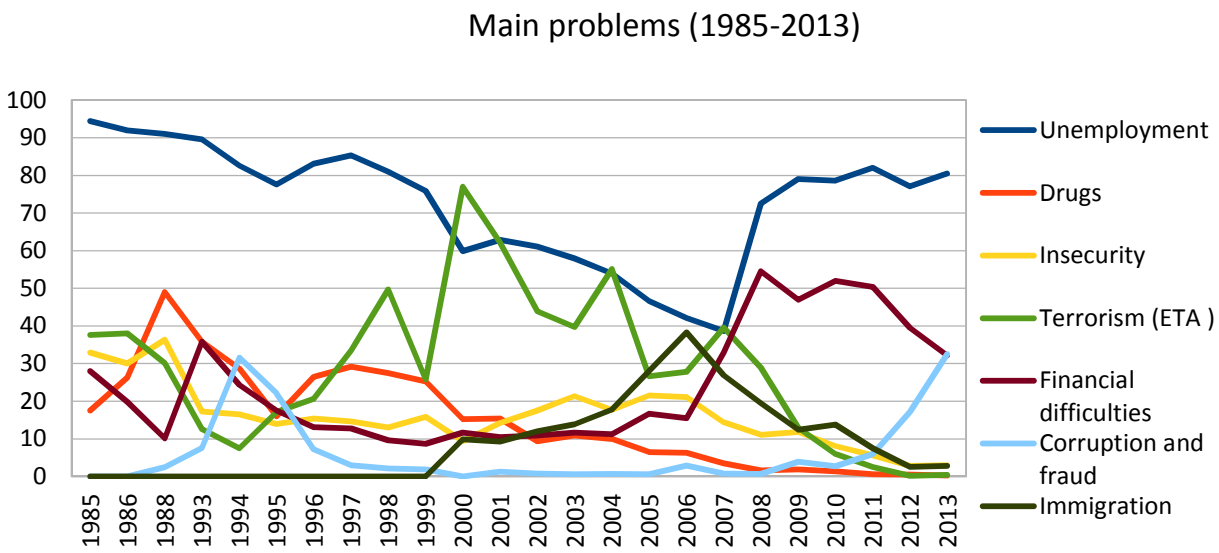
5.2 The geography of neighborhood watch

While neighborhood watch in Spain has never been a generalized phenomenon, citizen patrols have emerged repeatedly since the end of the dictatorship in 1978. The first patrols that we have identified appeared in the 80s and 90s in urban peripheries, mainly around Madrid, Barcelona and Valencia. Working-class neighborhoods with large number of internal migrants that arrived from rural areas to larger cities looking for work formed the so called 'pickets of self-defense' [piquetes de autodefensa]. Neighborhoods without many public services where citizens felt 'abandoned' by the Administration´s 'negligence'. These were also the areas where the heroin pandemic hit the hardest, and so trafficking, drug abuse and drug-related crime were common and for all to see. With the development of Spanish democracy, services slowly arrived to these areas and, coinciding with a global trend, heroin consumption receded –and so did the citizen patrols.

In the late 90s and early 2000, neighborhood patrols reappear in the media. This time, however, in slightly new scenarios –neighborhoods with high rates of migrants from the Global South. The motivation for residents to self-organize to protect their areas was very similar to those of the 80s, namely to end drug dealing, prostitution, youth gangs and antisocial behavior. But this time the migrants were not the actors but the 'deviant', the object of surveillance. We have identified such schemes in the neighborhoods of Raval in Barcelona, Legazpi in Madrid and in Mariana, in the city of Valencia.

Urban patrols do not appear again in the press after 2005. However, we have found them in rural areas and in residential developments of single-family homes or chalets, away from the

urban centers, where public services are scarce. We have found these in the Alicante area, where residents organized themselves and formed patrols to protect their homes from theft.



Especially since 2007, when the economic crisis started, farmers and ranchers began to be victims of larceny in their houses and farms. Their tools, electrical material, copper tubing, systems of irrigation, machinery, crops, diesel oil, livestock, etc. were being stolen and groups of farmers organized patrols, sometimes with the support of local authorities, in the areas of Lleida, Andalucía, Extremadura and Castilla.

We observe that due to changes in crime patters, crime watch schemes in Spain have gone from cities to farmlands, from urban peripheries to rural and unpopulated areas.

5.3 The sociological perspective

On order to understand the emergence of patrols it may be useful to review the relevance of insecurity issues among the population's concerns. The sociological surveys of the Spanich Centro de Investigaciones Sociológicas (CIS) ask citizens on a monthly basis what their main concerns are. Despite the limitations of this type of study, it can give us an idea of the evolution of the problems that the Spanish society has referred to as more important. When looking at the figures, it is important to bear in mind that Spain has suffered from chronic unemployment and the activities of a terrorist organization, Euskadi Ta Askatasuna (ETA).

Source: own elaboration using CIS data

In order to facilitate the understanding of these data and to establish if there is any relationship with the neighborhood watch phenomenon, we have chosen to analyze the data in three sets of 10 years (coinciding with the emergence of the different types of patrols presented in the previous section).

Between 1985 and 1995 the main problem of Spanish society was, by far, unemployment. The second was drugs. Sky-high unemployment rates recorded during those years, as a result of the economic downturn of the 1980s, severely affected the working-class neighborhoods of urban peripheries, especially young people. These neighborhoods became the focus of drug-related social problems -particularly heroin addiction. ETA, insecurity and financial difficulties also appear as problems, and the concern over 'security' peaked in 1988. In was precisely around this time that the press records the emergence of neighborhood patrols in cities like Bilbao[851] and La Malvarrosa (Valencia).[852] Shop keepers in a Madrid district, Aluche, organized night patrols to prevent theft,[853] and in San Roque (Algeciras) neighbors organized patrols to prevent drug trafficking.[854]

Drugs were perceived by society as a source of insecurity and problems, but the ones who suffered most of its consequences were the districts in urban peripheries, where the police rarely patrolled while the neighbors witnessed hustling, robberies (to people and businesses), drug consumption in public areas, etc. In 1991 there were episodes in which drug users were physically expelled from certain areas, and the press and the authorities harshly criticized these extremes and the means used by citizen patrols. After these

[851] 'Alzamiento vecinal contra la droga', El País, November 27, 1987. Available at http://elpais.com/diario/1987/11/27/espana/564966032_850215.html
[852] 'Los intocables de la Malvarosa', El País, November 29, 1987. Available at http://elpais.com/diario/1987/11/29/espana/565138820_850215.html
[853] 'Comerciantes de Aluche organizan patrullas nocturnas para evitar robos', El País, January 8, 1988. Available at http://elpais.com/diario/1988/01/10/madrid/568815856_850215.html
[854] 'Vecinos de un barrio de San Roque patrullan para impedir el tráfico de drogas', El País, June 13, 1999. Available at http://elpais.com/diario/1989/06/13/espana/613692026_850215.html

controversies, a Community safety Law was passed in 1992, allowing more police discretion and harsher sentencing for certain offences. In 1993 the Spanish economy started to recover and unemployment started to decrease, as did financial difficulties.

Between 1996 and 2004 the conservatives gained office in Spain, for the first time since the end of the dictatorship. During this period, terrorism became the citizen´s main concern, due to several high-profile cases of kidnap and murder. However, between 2000 and 2003 concern for insecurity increased again. As we saw earlier, in this period crime rates increased, as did the emergence of international migration as a perceived security problem. In 1991 Spain had a positive migratory balance for the first time in the 20th Century, and while the weight of migrants in the total percentage of the population was still low, the novelty of the phenomenon made it more visible. By 2005, however, the figures of 1991 had increased by 1,000% (from 350,000 to 3,690,000 registered foreign-born residents). The press and politicians did not hesitate to grossly link immigration and crime,[855] and some neighborhood patrols replicated this racist discourse and organized to throw out prostitutes, smugglers and gang members, especially when they were foreigners.

In the last period, 2005 to present, the economic crisis and the burst of the housing bubble substantially modified the priority of problems suffered by Spanish society. We observe an increased concern about unemployment, financial difficulties and corruption, which runs parallel to the decrease of terrorism after ETA's ceasefire in 2010. Even though immigration and insecurity are no longer considered major problems during this period, 2005-6 constitute an exception to this trend. In those years, the media tended to link migration with insecurity in its coverage of violent assaults to houses, pointing to an increase in the presence of organized gangs of foreign criminals. These assaults were mostly concentrated in Catalunya

[855] For example: 'The Government blames the increase in crime to immigration and ease to denounce', El País, February 11, 2002; 'Ana Botella links rising crime with the influx of immigrants', El País, February 6, 2003), or 'The Ministry of the Interior includes the detention of foreigners without legal papers as part of their plan against crime', El País, March 8, 2003.

(in rural areas) and Alicante (in residential suburbs), and in some cases patrols emerged to demand more police protection.[856]

On the basis of this analysis, we can establish that while citizen´s patrols respond to local circumstances, these also show a robust relation with society's main concerns overall. As we have seen in the previous section, crime rate has remained fairly stable in recent decades, and so while it is difficult to establish a connection between crime rates and the emergence of neighborhood watch schemes, we do observe a link between the patrols and concern over insecurity, drug abuse, migration and the economic crisis, which are the major problems perceived by the Spanish population.

5.4 Stakeholders: police, members, media, authorities and the critical public

5.4.1 The Police

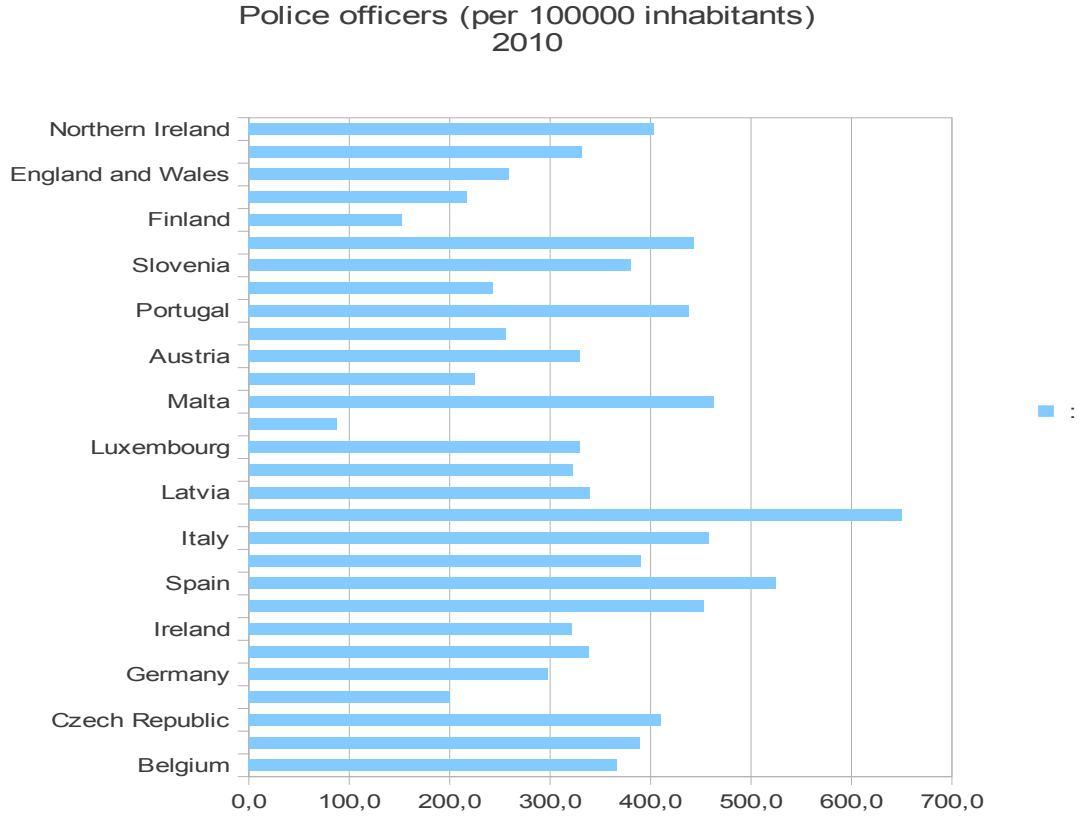
The police has reacted negatively to the formation of neighborhood watch schemes, and neighborhood watch members often complain in the press that the police prevent them from doing their job. In the 80s, the police often had to defend prostitutes and drug users from the patrols. In October 13, 2000, the press reported that 'local and state police is deployed in the neighborhood, advising prostitutes to leave or hide', and neighborhood watch members were sometimes arrested.[857] However, we have also found cases of cooperation and collaboration between the police and vigilantes or patrol members, especially in rural areas and in small towns that do not have a local police force.

In most cases, the patrols demand more police presence and do not intend to substitute the police force. In fact, it is not uncommon for neighborhood watch initiatives to make explicit

[856] 'Vecinos de La Marina Baixa amenazan con comprar armas', El País, May 10, 2005. Available at http://elpais.com/diario/2005/05/10/cvalenciana/1115752700_850215.html
[857] 'Los vecinos patrullan las calles contra la prostitución y la droga en los barrios de El Grau y la Malvarrosa', El País, October 13, 2000. Available at http://elpais.com/diario/2000/10/13/cvalenciana/971464677_850215.html

that they will cease their activities the moment they see more police presence in their areas.[858]

On the other hand citizens organized patrols to demand more police control and announced that their mobilizations would be suspended when they felt they were being protected by more police officers. It is therefore relevant to address whether there is a lack of police in Spain, as the demands of the patrols would indicate that that is the case. If we compare the number of police officers in Spain to the rest of the EU, this does not seem to be the case, as Spain is the second country in the EU with a higher turnover of police officers, only behind Cyprus.



[858] 'Las patrullas' de Ciutat Vella dejarán de salir a la calle si ven más policía', El País, July 20, 2000. Available at http://elpais.com/diario/2000/07/20/catalunya/964055238_850215.html

5.4.2 Neighborhood watch members

The citizen patrols in Spain are usually organized by neighborhood associations, groups of residents organized to address specific problems, groups of shop owners and small businesspeople, farmer unions and, in some small villages, by the local authorities. On the basis of the press coverage and the interviews conducted, we can establish some features of the members that have integrated these patrols.

In the 80s and 90s the patrols were integrated mainly by workers of different ages, and what some identified as the 'social base of the left'.[859] These were patrols that came out of the residents associations that campaigned for more public services (schools, hospitals, transport, etc.), and often organized themselves together with politicians to express their grievances. It is worth highlighting that in many cases their actions were aimed at raising awareness about the problems they faced, and these were approached in a sensible manner, by organizing campaigns or actions such as the cleaning of flats used by drug users, in order to get attention.[860] While most of the neighborhood patrols of the time were peaceful and campaigned for public security as part of a broader initiative, some of them were also very violent and reflected the contradictions and tensions of the time.

There were also instances when the neighborhood associations criticized the actions of the patrols. In Barcelona, they published a manifesto against an initiative to patrol the streets of the Raval area.[861] In all these instances, as we found for later years, the members of the patrols came from low-income families and were usually residents in the neighborhood. In some instances, however, we found newcomers joining the schemes.[862]

---

[859] 'IU reconoce que las patrullas se nutren de la base social de la izquierda', El País, January 14, 1991. Available at http://elpais.com/diario/1991/10/14/espana/687394801_850215.html
[860] 'Vecinos de Leganés adecentan un piso de "yonquis· porque el servicio municipal se negaba a limpiarla', El País, October 24, 1991. Available at http://elpais.com/diario/1991/10/24/madrid/688307056_850215.html
[861] 'Las patrullas se quedan solas', El País, August 29, 2000. Available at http://elpais.com/diario/2000/08/29/catalunya/967511248_850215.html
[862] 'Patrullas "antidroga" en Legazpi', El País, September, 14, 2001. Available at http://elpais.com/diario/2001/09/14/madrid/1000466654_850215.html

Finally, from 2005 onwards, when the emergence of the patrols was related to robberies in rural areas, the social composition of the neighborhood watch schemes changed. These rural schemes, which usually patrol in vehicles, are mainly integrated by men over 50, often the owners of the land or property they are trying to protect.[863] In the case of rural patrols, trade unions and local authorities have played an ambivalent role, occasionally discouraging their creation, because of their *alegal* character, but also promoting them in some cases.

Despite the different characteristics of the groups that decide to organize patrols, we find that all neighborhood watch schemes have something in common –the predominance of men over women, with most initiatives being 100% male. Other than that, we can establish different characteristics for urban and rural patrols, as while the urban ones are composed mainly of working class men trying to protect their physical integrity; in the rural areas, the members are usually farm owners (not necessarily wealthy) who organize to protect their livelihoods. It could be argued that while the wealthy have the resources to install alarms, video surveillance and private security, other groups need to organize themselves in patrols to raise awareness about their perceived insecurity and get a response from the authorities.

5.4.3 The media

As pointed out by García and Pérez,[864] the construction of the social perception of crime is not determined exclusively by the existing criminal activity but also by the contribution of the media and the political debate. As Tuchman says, 'the act of producing news is more an act of constructing reality than reflecting an actual image of reality'.[865] In the case of crime and insecurity, this *performative* ability of the media is especially relevant, as this is a politically

[863] 'Por si acaso', El País, July 13, 2013. Available at http://ccaa.elpais.com/ccaa/2013/07/12/catalunya/1373654232_496488.html
[864] GARCÍA ESPAÑA E. and PÉREZ JIMÉNEZ F. (2004). "Evolución de la delincuencia en España y Andalucía: Análisis e interpretación de las estadísticas oficiales". Málaga: Instituto Andaluz Interuniversitario de Criminología y Fundación El Monte. Pg. 5.
[865] TUCHMAN, G. (1983) *La producción de la noticia. Estudio sobre la construcción social de la realidad*. Barcelona: Ediciones Gustavo Gil. Pg. 24.

sensitive subject that can mobilize large numbers of voters to demand more punitivism.[866] When the media cover a specific crime event, they create an 'information wave'[867] that can lead to a moral panic.

Coverage of neighborhood patrols by the media has shifted over time. In the 80s and early 90s, with the Socialists in power, the newspapers tended to highlight the brutality of such initiatives, with headlines such as 'Beating',[868] 'Justice into their own hands',[869] Neighbors try to lynch a man who was doing drugs,[870] 'Anti-drug patrols wound 26 people in Barcelona',[871] 'Armed with sticks, chains and umbrellas, groups guard their street every day'.[872]

In the second period, after the conservatives gained power (1996), the media focused more on the motives of the patrols than their methods, and the headlines changed from alarm to explanaition –'Riuclar threatens to create neighborhood patrols against insecurity',[873] or, under the descriptive 'Citizen patrols in Castellón' headline, a news piece described how insecurity had become a problem that needed attention, and echoed the residents' demands. It could eb argued that in this second period the media became an 'ally' of the patrols' members, as their description of neighborhood grievances worked as a loudspeaker for their demands.

Overall, we have found that neighborhood patrols have often been both overrepresented and distorted in the Spanish media. Overrepresented because while the instances of citizen

[866] FUENTES OSORIO, J.L. (2005) "Los medios de comunicación y el derecho penal", en *Revista electrónica de Ciencia Penal y Criminología*. Pgs. 7-16.
[867] SOTO NAVARRO, S. (2005) "La Influencia de los medios en la percepción social de la delincuencia", en *Revista electrónica de Ciencia Penal y Criminología*, , 7-9. Pg. 6 onwards.
[868] 'Apaleamiento', El País, January 17, 1987. Available at http://elpais.com/diario/1987/01/17/espana/537836409_850215.html
[869] 'La justicia por su mano', El País, February 3, 1988. Available at http://elpais.com/diario/1988/02/03/opinion/570841212_850215.html
[870] 'Unos vecinos intentan linchar a un hombre que se estaba drogando', El País, June 21, 1991. Available at http://elpais.com/diario/1990/06/21/madrid/645967458_850215.html
[871] 'Las patrullas antidroga causan 26 heridos en un barrio de Barcelona', El País, October 7, 1991. Available at http://elpais.com/diario/1991/10/07/portada/686790001_850215.html
[872] 'Grupos armados con palos, cadenas y paraguas vigilan cada día su calle', El País, April 20, 1993. Available at http://elpais.com/diario/1993/04/20/madrid/735305058_850215.html
[873] 'Riuclar amenaza con crear patrullas vecinales contra la inseguridad', El País, November 1, 2001. Available at http://elpais.com/diario/2001/11/01/catalunya/1004580457_850215.html

patrols in Spain have been few and far between, they have always received a remarkable degree of media attention. Related to this overrepresentation, they have also been distorted.

On the one hand, the media have tended to simplify the problems and the actors involved in neighborhood patrols, especially those allegedly responsible for the feelings of insecurity – 'junkies', street sellers (mostly Roma), migrants (often organized in gangs) and prostitutes. As Bergalli points out "the mass-media not only determines (to and for the people) what significant facts have taken place but they also point out how are they to be understood'.[874] Regarding the relationship between robberies in homes and organized gangs, for instance, on May 28, 2005, the newspaper La Vanguardia published an article with the headline 'New laws for new crimes' with a daunting subtitle: "From now on, it will be possible to prosecute and sentence entire gangs, as if they were terrorists'. The article pointed out the possibility of including 'organized crime' in the Penal Code in order to treat certain type of criminal actions as terrorist crimes so that any member of the band would receive the same criminal punishment, regardless of their level of participation in the crime.[875]

Recently, a newspaper covered the use of drones by rural patrols in Tarragona and Girona.[876] While the headline used the future tense and made it look as if it was a fact, with a picture of people using drones in a rural area, a careful read of the piece revealed that a private company was offering drones and synthetic DNA to farmers as a way to combat crime –but no drones had been purchased to be used by neighborhood watch members yet, nor were the people depicted in the article members of one. Moreover, according to a police representative, the rural patrols in Tarragona had not actually patrolled at the time of publication.[877]

---

[874] BERGALLI, R. (1983) *Perspectiva sociológica: sus orígenes,* in BERGALLI, R., BUSTOS RAMÍREZ, J. And MIRALLES, T., *El pensamiento criminológico: Un análisis crítico*. Barcelona: Ed. Península. Pg. 53.

[875] ?Nuevas leyes para nuevos delitos', La Vanguardia, May 28, 2006. Available at http://hemeroteca.lavanguardia.com/preview/2006/05/28/pagina-35/49005293/pdf.html

[876] 'Els pagesos de Tarragona i Girona vigilaran les finques amb drones', El Periódico, December 28, 2013. Available at http://www.elperiodico.cat/ca/noticias/societat/els-pagesos-tarragona-girona-vigilaran-les-finques-amb-drones-2962951

[877] Interview with the Superintendent of the West Police Region (Lleida). December 2013.

Image published by *El Periódico* on December 28, 2013. Source: www.elperiodico.cat

5.4.4 The authorities

The way the authorities have reacted to the emergence of citizen patrols is a good indicator of how politicized has this phenomenon become. The local authorities in the municipalities where neighborhood watch schemes have been organized have taken very different stances. Depending on the degree of local responsibility in relation to the problem of community safety, their means and their political tendency (as well as their relation with the political tendency of those leading the patrols or the State authorities), the local authorities have promoted and legitimized the patrols, joining their members in exposing insecurity or the issues raised by the patrol members; or they have delegitimized and criminalized their leading members.

On the one hand, we have found Town Halls that support and even convene the watchers.[878] This is mostly the case in small, rural towns without local police. In such cases, the Mayor joins other citizens in supporting the initiative to patrol certain areas with the aim of increasing its ability to provide security, to react to specific criminal developments such as an increase in property offences or to put pressure on state actors to increase the police budget for their area.

On the other hand, in big cities, where the local authorities have greater competences related to security as well as their own local police force, Town Halls tend to be critical about the emergence of citizen patrols, call on their members to dissolve them and highlight their alegal character.

Overall, we observe that the formation of neighborhood watch schemes has been an instrument for political pressure. The citizens that self-organize to patrol the area where they live are critical of the way security is provided by the competent authorities. Therefore, when the local and state/regional authorities do not share their party affiliation, the patrol is used as an excuse to criticize the next level of government. When they do, neighborhood watch schemes are heavily criticized.

5.4.5 The critical public

As mentioned above, insecurity and crime are a major concern among the Spanish population. While crime in Spain is not high, there is a correlation between perceived insecurity and the emergence of neighborhood watch schemes. However, the lack of support for such schemes is remarkable, and could be attributed to their exceptional character, their alegal character, the danger involved in being an active participant at a time of conflict or even their high degree of politicization. This could also be due to the fact that every time the

[878] 'Juventudes Socialistas promueve patrullas de vigilancia ciudadana en Camponaraya', leonoticias, May 1, 2012. Available at http://www.leonoticias.com/frontend/leonoticias/Juventudes-Socialistas-Promueve-Patrullas-De-Vigilancia-Ciud-vn97962-vst208

patrols make headlines or the authorities suggest that they could be tolerated, a reaction is perceived in the form of letters to the editor, op-eds and even editorials that voice a generalized concern over the privatization of security provision and the unintended consequences of legalizing such schemes and their understanding of security and insecurity. This was specially the case I the 80s and 90s, when the violence, brutality and racist character of some of the neighborhood watch members was covered in the press.[879]

Also, most community associations at the neighborhood level, with a strong tradition in Spain and very active in the 80s and 90s in the demand for public services at the local level, have been very outspoken against such schemes, exposing that they are usually led by a handful of individuals with very weak ties with the community and without a true broad support for their demands and actions. Specially in those years, it is worth highlighting that the neighborhood watch form was not even favored by some of its members, who would complain about the cost in time and rest implied in taking part in a patrol and so used their actions as a strategy to get the authorities to react to a perceived lack of security services and responsiveness by the local administration –but not with the aim of replacing the police or being a permanent subsidiary force.

Therefore, while the demand for security is strong, the methods used by the patrols are usually met with distrust by most neighbors and parties involved.

6. Toward a typology of 'traditional' neighbourhood watch in Spain

As we have established in the previous sections, in the last 30 years various types of patrols have emerged at specific moments and spaces and with different objectives. While the legal framework in Spain has not allowed for the emergence of a 'typical' neighbourhood watch

[879] See, for instance, 'La justicia por su mano', El País, February 3, 1988 or 'Problema real, respuesta equivocada', El País, October 11, 1991.

model, we can distinguish four broad patrol types according to their geography, sociology and relation to crime and disorder:

	Places	Crime related to the patrol´s development
1980-1995	Low income neighborhoods in urban peripheries	Insecurity related to drugs, robberies, antisocial behavior, etc.
1996-2004	Derelict inner-city neighborhoods	Insecurity related to antisocial behavior, immigration, prostitution, gangs, etc.
2005-2006	Suburbs	House robberies
(2002); (2006) 2010-2013	Farms and rural areas	Theft of diesel oil, tools, equipment, electrical materials, copper pipes, machinery, crops and livestock.

Four categories of neighborhood watch in Spain. Source: own elaboration.

Despite the differences, these patrols have certain common characteristics. They always emerge after a ‘shock’ experienced by the community, related to some kind of criminal activity. While feelings of insecurity can be fostered by the media and the political discourse, we find that in Spain ‘traditional’ citizen patrols have been the result of a very close or direct victimization.

On the other hand, in all cases we have found a feeling of ‘abandonment’ expressed by the patrols’ members, a sense of ‘second-class’ citizenship, of being ‘forgotten’ and feeling vulnerable to attacks. The patrols reveal a need to be listened to.

The same time, as we observed earlier, in most cases patrol members come from low-income, working class families and neighbourhoods. Even in the case of rural patrols, these are integrated by small farm owners. Our assumption is that getting organized and demanding more protection from the government by means of substituting the police is the resource of the resource less, as those who can afford it have other means at their disposal, such as private security, surveillance technologies and political capital to have their voices heard.

However, at the individual level, we have found two cases where the motives of some of the neighbourhood watch leaders have become a problem –due to their need for protagonism or personal hidden agendas. Specifically, this has been raised by two interviewees in relation to the urban patrols in Barcelona around the year 2000 and rural 'somatens' in 2010-2013.[880]

On the whole, citizens who integrate neighbourhood watch schemes in Spain do not wish to assume the responsibility for their security on a permanent basis. Patrols are extreme emergency measures undertaken to draw the attention of the authorities, and wee have found no intention to 'privatize' the provision of security –quite on the contrary, both supporters and opponents of such initiatives, bar some individual cases, share a reluctance to accept a private involvement in security provision and policing functions.

Nonetheless, the citizen patrols have played a role in changing the Spanish legal landscape and toughening the Penal Code to respond to a growing pressure about rising feelings of insecurity. While we cannot establish a direct relationship between the emergence of the patrols and legal changes, the ability of neighbourhood watch to be echoed in the mainstream media leads us to believe that these schemes are relevant to understanding how security and criminal policy have changed in Spain over the last 35 years.

We have summarized this hypothesis in the following table:

[880] Interview with Barcelona's Councilor for Community Safety at the time. April 2010; Interview with the Superintendent of the West Police Region (Lleida). December 2013.

	Crime linked to the emergence of neighborhood watch	Laws	Legislative changes
1980 - 1995	Insecurity related to drugs, theft, etc.	Organic Law 1/1992, On the Protection of Community Safety	- More police discretion. - Identifications and possibility of detention. - Punishment for drug consumption in public areas.
1996 - 2004	Insecurity in neighborhoods with high immigration rates, prostitution, gangs, etc.	Organic Law 11/2003, on specific measures for community safety, domestic violence and the social integration of foreigners	- Aggravation by recidivism (‘three strikes and you are out-style). - Expulsion of non-residents sentenced to less than 6 years in prison
2005 - 2006	Theft in suburban homes	Organic Law 5/2010, modification of the Penal Code.	- The figure of Criminal Groups and Organizations is created, even when these are not permanent. The figure of Transient Association to Commit a Crime is created in order increase jail time for those involved in break-ins. -Recidivism: six to eighteen months of

			incarceration for car burglars who repeat the crime in one year if the amount stolen is greater than 400 euros.
2002 2006 2010 - 2013	Theft in rural areas and farms	Proposal for a change in the Penal Code	Modification of Art. 235 of the Penal Code - Aggravation for the penalty of theft (one to three years in prison) when it involves stealing pipes, wiring, equipment or infrastructure components for power supply or telecommunication services; or agricultural and livestock products, instruments or means used to obtain these, provided that the crime is committed in agricultural farms.

7. The other neighborhood watchers: internet and dissent

While most people's idea of what a neighborhood watch is has been covered in the previous section, there are two relevant developments that require some further exploration. One is part of a shared trend and is linked to the increased use of the internet, ICTs and other technologies. The other is apparently specific to the Spanish case, and it can be attributed to the fact that the lack of legal coverage for neighborhood watch schemes in Spain has meant that different typologies of patrols have emerged. These function in similar ways as regular schemes in the sense that they organize citizens that are concerned by something that is

happening around them and involves their sense of insecurity and/or vulnerability, but their ends and logic are very different from those of traditional neighborhood watch experiences.

7.1 Technology-intense neighborhood watch: 2.0 & drones

New technologies and digital media mean that vigilantes can now go online. There are already several examples of neighborhood watches using social media to communicate, or instances of crowdsourcing the act of 'watching'. The most well-known example is probably Blueservo,[881] a project first proposed in 2006 with the intention of 'crowdsourcing' the policing of the US-Mexico border and 'empower[ing] the public to proactively participate in fighting border crime' –that is, reporting on migrants trying to enter the US. Another example would be 'Internet Eyes',[882] where pre-registered grasses get access to real-time footage from cameras installed in different setting, and receive cash rewards in case of 'positive alerts'.

Not all crowdsourcing is CCTV-based, however. In 2010 a, English-speaking Barcelona resident launched a website and Facebook page called 'Robbed in Barcelona' in order to 'raise awareness of the situation in Barcelona, but more so to embarrass the local authorities into action'.[883] The site encourages people to anonymously send pictures, videos and tips on pickpockets and thieves in Barcelona, and there are frequent stories of robberies detailing methods and the physical appearance of those identified as perpetrators. While some comments are just descriptions or laments for things that have happened, others tell stories that are quite hard to believe:

[881] See http://www.blueservo.net/
[882] See http://www.interneteyes.co.uk/
[883] See http://www.robbedinbarcelona.com/2010/03/09/the-creation-of-robbed-in-barcelona/

This is not the only instance of 'foreign' watchers going online. The only example of a neighborhood watch with an online presence similar to what is found in other European countries is called 'Vecinos Cooperando. Neighbourhood Watch in Spain'[884] and it serves the Alicante area. Interestingly, the website is in English and all contributors have English-sounding names, which points to an interesting case of policy transfer -but also to the fact that online tools might be a useful resource for communities that are not fully integrated in their local context and do not have the numbers or the physical space to relate otherwise.

But foreign residents are not the only ones to use ICT. In 2013 a so-called 'somatén' in a town of 2,000 people, Riudellots de la Selva, launched a Facebook group and a 'whatsapp' account that members use to exchange tips and pictures of any abnormal activity they spot.[885] The contributions are a mixture of self-promotion, dissemination of relevant news pieces, comments about specific crimes that occur and stories about people begging, looking for a place to squat or just wandering around in the village. The information that is shared does not seem to be a contribution to an offline dynamic, but a fully online experience which may or may not translate into a 'physical' scheme if the community experiences an episode of stress related to security.

Finally, as mentioned above, a regional paper recently reported that some rural neighborhood watch schemes are planning to use unmanned aerial vehicles equipped with high-resolution thermal imaging cameras and night vision. While the wording of the news

[884] See http://www.nhwinspain.com/
[885] Facebook page available at https://www.facebook.com/sometent.riudellotsdelaselva?fref=ts

piece revealed that this is just the vision of the company trying to sell the drones to members, it is quite likely that this will become a reality in the near future.[886]

In all these instances, images of specific individuals (personal data) are or will be circulated without permission, consent or registry, and we have found no evidence that such schemes actually contribute to the reduction of crime or fear, beyond providing a space to share experiences, tips and a sense of protection.

7.2 Tales from the other side: Neighbourhood care, counter-patrols and policing the police

Often times there is a thin line between neighborhoods watch schemes and vigilantism. Even when citizen patrols are intended as a civil contribution to people's safety, the impact of prejudice and racism on the way these schemes create the 'other' that needs to be watched is difficult to ignore, as the link between migration and patrols shows. Also, as the neighborhood watch schemes against drug use from the 80s show, even when integrated by working class people who rightfully feel that insecurity impacts their quality of life and that of their children by putting them at risk, it is always easier to chase a drug user than a drug dealer. Those watched and chased by patrol members are always the most vulnerable in their own ways –victims of a drug addiction, victims of women trafficking or exclusion in the case of prostitutes, and so on.

However, there are also examples of neighborhood watch-like schemes that defy this definition and explore the solidarity components of self-organizing to defend the community. As the website 'Robbed in Barcelona' shows, petty theft is common in Spain. Often times it is older people that are most affected by these kind of offences, as they are the most

[886] 'Els pagesos de Tarragona i Girona vigilaran les finques amb drones', El Periódico, December 28, 2013. Available at http://www.elperiodico.cat/ca/noticias/societat/els-pagesos-tarragona-girona-vigilaran-les-finques-amb-drones-2962951

vulnerable when attacked after withdrawing money from a cash machine or when running errands with their jewelry on. It isn't difficult to imagine that many old people manage to make ends meet and dare to go outside after an attack thanks to the help and solidarity of family, friends and neighbors.

There are few accounts of these informal networks of solidarity, but community groups mention that it is common for volunteers to accompany older people when they go out to do their shopping, visit the doctor or spend some time at a community center.[887] In a middle-sized town in Catalunya, Reus, neighborhood residents have organized themselves to help elders who have been attacked to go back to their normal lives by meeting them on a regular basis to go out in the streets and regain the confidence lost after an attack. Contrary to the examples mentioned so far, these groups do not seek media attention nor have specific demands to make to the authorities. They see their schemes as a way to do the right thing and get involved in what happens in their neighborhoods, and while some members do mention migration as a reason of recent neighborhood decay, a racist discourse does not seem to have emerged from such initiatives.[888]

Neighborhood care schemes are not the only examples of neighborhood watch that escape the link with vigilantism. In the Andalusian capital, Seville, several groups got together in the summer of 2011 to raise awareness on some situations which they felt were the result of the lack of policing, such as the growing number of informal 'parking attendants' that make a living by requesting a tip from drivers who want to leave their car in specific areas, or the shanty towns established in the outskirts of the city and inhabited mainly by people of a Romanian origin. These patrols were quickly dismissed by some of the more established

[887] Interview with community worker. May 2013.
[888] 'Abuelos con escolta', El Periódico, May 6, 2013. Available at http://www.elperiodico.com/es/noticias/sociedad/abuelos-con-escolta-2392041

neighborhood associations and the authorities, and some radical organizations exposed the links between some of their members and the fascist far right.[889]

As members of these patrols decided to gather regularly in different shanty towns and to harass parking attendants, some groups affiliated to the local radical left decided to organize 'contra-patrullas' and to meet at the same time and place as the members of the neighborhood watch to force them to dismantle the scheme, with a degree of success, as the tweet written by a member of the counter-patrol and captured on February 23th shows.[890]

According to a member of the counter-patrols, this initiative has managed to stop the 'racist' initiative by convening at the same time and place, but also by going to their assemblies and arguing against it, as part of a broader political effort to stop racism and fascism in the area.[891]

A similar development occurred in Madrid when activists felt some members of the central neighborhood of Lavapiés were being harassed due to their looks and origin. This time, however, the profiling was not done by other citizens but by the police.

Police profiling is Spain is pervasive and illegal, according to several sources.[892] Stopping people to conduct identity checks based on the appearance of those who 'do not look

[889] 'El ultraderechista Ángel Bordas, detrás de un nuevo brote xenófobo en San Jerónimo', Indymedia Estrecho, July 7, 2012. Available at http://estrecho.indymedia.org/sevilla/noticia/ultraderechista-angel-bordas-detras-un-nuevo-brote-xenofobo-san-jeronimo
[890] 'Xenophobic citizen patrol deactivated! Racists out of #Seville! #againstfascismnotonestepbackwards'
[891] Interview with a member of the counter-patrol in Seville. November 2013.
[892] See, for instance: http://www.opensocietyfoundations.org/press-releases/report-un-details-pervasive-ethnic-profiling-spain

Spanish' is a common procedure that has never been discouraged or punished by the police authorities, even if there is ample evidence that police profiling is discriminatory, racist and useless. In 2011, after the 15M movement abandoned the squares to continue its activities at the local level, the neighbors of Lavapiés decided to make the struggle against 'racist police raids' one of their main activities, even if there have been campaigns dating back to 2008. Since then, videos of police operations stopping people of migrant 'appearance' are regularly posted online,[893] and members of the community alert one another, via telephone, twitter[894] and other means, when this happens, and they try to inform people about their rights, to disrupt the raid and expose the racist character of this practice. The members of these 'Neighborhood Brigades to Observe Human Rights Compliance'[895], who identify themselves with orange waistcoats, meet regularly to organize and coordinate their actions, and involve people of all ages who are usually politically active in the left and social movements at the local level.[896]

[893] 'Redadas racistas en Lavapiés'. Video available at http://www.youtube.com/watch?v=7LcBRjc0sWk
[894] Twitter feed available at https://twitter.com/BrigadasDDHH
[895] Brigadas Vecinales de Observación de Derechos Humanos. Website available at http://brigadasvecinales-ddhh.blogspot.com.es/
[896] Interview with a member of the Neighborhood Brigades in Madrid. December 2013.

Members of a 'brigade' informing people about their rights at a metro exit in Madrid. Source: www.brigadasvecinales.org

According to their reports,[897] between May 2010 and November 2012, members of the brigades recorded 1,144 racist raids, and their members have faced harassment and legal action, including criminal charges for obstruction and disobedience. These brigades are probably one of the most long-lived and active instance of neighborhood watch in Spain, even if their activity is not what most expect when discussing neighborhood watch schemes.

These 'tales from the other side' exposes a counterintuitive picture, where community organizing and surveillance are used in ways that are more diverse to those allowed for by traditional neighborhood watch schemes. Interestingly, it is in these 'other' patrols that we find greater diversity in terms of the age and origin of the participants, even if in some cases the political affiliation of the members are more homogeneous than found in traditional schemes.

This points to interesting questions in terms of power, resilience and legitimacy, as in the non-typical examples we observe a 'blowback reaction' –the watched appropriate the ways and means of the watchers, and the hierarchy of control is subverted. Suddenly, a nation of grasses meets a nation of whistleblowers that uses the same social media, community rhetoric and appeals to the greater good to explain and justify its existence, even if their objectives and logics are very different. Both scenarios, however, point to an interesting tension between public and private, between bottom-up and top-down legitimacies and between watching and being watched.

[897] Controles de identidad racistas en Madrid. Informe de las Brigadas Vecinales de Observación de Derechos Humanos. Available at http://www.gugms.net/brigadasddhh/INFORME_BRIGADAS_2011.pdf

IRISS Work Package 3

Case Study: Neighbourhood Watch in the United Kingdom

Contribution by: STIR (Charles Leleux and William Webster)

18 December, 2013

1. Methodology and Research Ethics Procedures

1.1 Methodology

Reference materials for this contribution have been drawn from a literature review of the origins of neighbourhood watch, which grew as a societal and community based response to personal, property and neighbourhood or community safety concerns. References to academic literature have also been used to offer reasons for the apparent differences in the growth of neighbourhood watch between the United States of America (USA) and the United Kingdom (UK). Its growth in the UK is recorded from the early 1980's to the present day, and the changing focus of the purposes of neighbourhood watch is also detailed, with the current focus appearing to be less concerned with monitoring and reporting unusual activities in an area, and more concerned with giving advice to residents on how to increase their resilience in respect of online security, personal security and protection of their home. There is also a strong focus on partnership working, and using advice and services of third party providers, in the public, private and third sectors. Details of these partners and links to their respective websites have been supplied. Information has also been drawn from interviews conducted by STIR with neighbourhood watch co-ordinators, police officers and organisations involved in crime prevention and safer neighbourhoods, which took place through the IRISS Project, WP4, relative to the topic of crime prevention. The interviews were conducted using either face to face

meetings or by telephone. Information contained in the case study has also been drawn from meetings, telephone conversations and email correspondence with Neighbourhood Watch Scotland,[898] which is the co-ordinating body for neighbourhood watch in Scotland; the Neighbourhood and Home Watch Network[899] which is the co-ordinating body for England and Wales, and the Northern Ireland Policing Board[900] which, along with the Department of Justice and the Police Service Northern Ireland, are responsible for co-ordinating neighbourhood watch activities in Northern Ireland.[901] Thus, information concerning neighbourhood watch activities in all four of the home nations which make up the United Kingdom of Great Britain and Northern Ireland, have been included in the case study.

The structure of the case study has been prepared following the guidance issued by OU, the lead partner of the IRISS project, WP3, and adheres to the case study protocol. The case study has been written in the context of citizen: citizen, and from the perspective of primarily the 'watcher', as it has been very difficult to ingather useful information and insight from the perspective of the 'watched'. Similarly, the democratic values and surveillance practices have been considered from the perspective of the 'watcher'. Evidence of the existence of resilience has been provided as a key cross cutting theme within the case study. The main research questions have been addressed, relating to the legitimacy, accountability, governance and representativeness of neighbourhood watch; its current purposes and how these have been influenced by the changing priorities of the Police; the role which new media is playing in the transformation of neighbourhood watch; the relationship between crime figures, and the reasons for the existence of neighbourhood watch schemes in local areas, and finally evidence of any controversies in the development of neighbourhood watch in the UK. The case study has also been constructed taking into consideration the themes and research questions contained in the Theoretical Framework (IRISS Deliverable D2.4), which has been used in this respect as an over-arching document for the case study report.

[898] Neighbourhood Watch Scotland: http://www.neighbourhoodwatchscotland.co.uk/
[899] Neighbourhood and Home Watch Network for England and Wales: http://www.ourwatch.org.uk/
[900] Northern Ireland Policing Board: http://www.nipolicingboard.org.uk/
[901] The authors' gratitude is extended to Neighbourhood Watch Scotland, to the Neighbourhood and Home Watch Network for England and Wales, and to the Northern Ireland Policing Board for the invaluable assistance which they each have given in the compilation of this case study.

1.2 Research Ethics Procedures

Empirical information contained in this case study has been used from interviews conducted by the University of Stirling for the IRISS WP4, crime prevention topic. All interviewees were advised of the funder, co-ordinators and purposes of the IRISS project and were provided with a link to the project website. They were also given the opportunity of asking questions in advance of the interview, prior to and at the conclusion of each interview. All interviewees were advised that their personal information would not be disclosed in the accounts (transcripts) of the interviews and that all persons' names and references to geographical locations where they live, work or have engaged in neighbourhood watch, crime prevention or community safety activity would be removed to ensure anonymity.

2. Historical Development of Neighbourhood Watch in the UK

2.1 Introduction

The first Neighbourhood Watch scheme in the United Kingdom has been widely reported as having appeared in Mollington, Cheshire in 1982[902] [903] with many commentators having argued that the early United Kingdom schemes were modelled on those which were in use already in the United States of America.[904] Other commentators report that the growth of neighbourhood watch in the United Kingdom was attributable to the eagerness of the British Police in following the lead of their American counterparts who saw advantages in encouraging communities to take more

[902] King, Michael, Social crime prevention a la Thatcher, The Howard Journal of Criminal Justice, Wiley Online Library, 28, 4, 1989, pp. 291-312.
[903] Tilley, Nick, The development of community policing in England: networks, knowledge and neighbourhoods, John Wiley & Sons, Ltd., Chichester, UK , 2008, p.98.
[904] Yarwood, Richard and Bill Edwards, Voluntary action in rural areas: the case of neighbourhood watch,
Journal of Rural Studies, 11, 4, 1995, Elsevier, pp. 447-459.

responsibility for their own safety, as a means of reducing the costs of policing.[905] The original concept of neighbourhood watch is claimed by some as having grown as a community-based response to the murder of Kitty Genovese in New York in 1964[906] in which a young woman was raped and murdered, and despite her cries for help (for around 30 minutes) having been heard by more than 30 neighbours, nobody apparently summoned help for her or went to her aid. The inaction of the bystanders in this murder led to the development of studies of the notion of 'bystander intervention' or 'bystander non-intervention'[907] [908] a feature of which it is claimed is that people acting as part of a group are less likely to intervene in such a situation as would an individual acting on their own. However, the origins of neighbourhood watch in the United States of America are probably not just due to the inactivity of the bystanders in the Kitty Genovese murder, but are more likely to be attributable to a number of other factors, such as the generation of a range of societal responses in seeking to protect homes, apartments, passengers on underground transport systems etc.,[909] or as a response, as Titus suggests, to the 'burglary epidemic' in the United States.[910] What is clear though is that in the context of the United Kingdom, the phenomenon of neighbourhood watch has, at different times, experienced significant periods of growth and contraction from its inception in the early 1980's. Today, neighbourhood watch is still continuing, albeit in different forms, with newer and more evolving purposes than before, often involving humanitarian and caring responses, including the widespread use of new social media, and with activities taking place with an increasing variety of different partners, from the public, private and third sectors.

---

[905] Bolton, Sharon, Crime prevention in the community: The case of Neighbourhood Watch, Taylor & Francis,
2006, p.40.
[906] Platt, John, Social traps, American Psychological Association, 28, 8, 1973, p.641.
[907] Levine, Mark, Rethinking bystander nonintervention: Social categorization and the evidence of witnesses at the James Bulger murder trial, Human Relations, Sage Publications , 52, 9, 1999, pp.1133-1155.
[908] Shotland, R. Lance, Lynne I. Goodstein, The role of bystanders in crime control, J.Soc.Iss., 40, 1, 1984, 1984, Wiley Online Library, pp.9-26.
[909] Bennett, Trevor; Katy Holloway, David P. Farrington, Does neighborhood watch reduce crime? A systematic review and meta-analysis Journal of Experimental Criminology, 2, 4, 2006, Springer, pp.437-458.
[910] Titus, Richard M., Residential burglary and the community response, Springer, 97, pp.97-130.

The context of the case study is that of citizen: citizen, and the analysis has been provided from the perspective of primarily the 'watcher' as it was very difficult to gain any meaningful information from the 'watched'. Surveillance undertaken by neighbourhood watch in the UK is non-negotiated, as the activities undertaken are decided by the 'watchers', although sometimes this is carried out in conjunction with other partners or stakeholders. The surveillance power relationship is therefore top down from neighbourhood watch to the local community, to specific individuals, or to certain spaces, and this may be happening without general public awareness, or individuals' knowledge or consent. It is difficult to provide an overall picture of the transparency or opaqueness of neighbourhood watch activities, as how each scheme operates will differ from area to area. The accountability, representativeness, governance and the existence of a democratic deficit surrounding neighbourhood watch schemes is examined in later chapters; the extent to which 'resilience' emerges as a key factor in the rapid expansion and apparent popularity of neighbourhood watch schemes in the UK is also addressed; the role which new media and surveillance technologies are playing in the transformation of neighbourhood watch is discussed, as is the existence of controversies in the development of neighbourhood watch, and finally an overview is provided on the changing role of the Police in relation to neighbourhood watch and community policing.

2.2 Growth and Spatial Distribution of the Schemes

Neighbourhood watch schemes, (or Home Watch schemes as they are sometimes referred to in parts of England and Wales), are active across all parts of the UK, which includes Scotland, England, Wales and Northern Ireland. Schemes in their totality cover a significant section of the overall population, as statistics supplied by the British Crime Survey demonstrate. They estimated that, in 2006/07 '…… 16 per cent of households currently belong to a Neighbourhood Watch scheme (this equates to an estimated 3.8m member households in England and

Wales).'[911] The reasons for creating (and the impetus for sustaining) these schemes can vary depending on localised and socio-demographic factors such as: the social classification and category of deprivation of the 'area'; levels of criminal activity; existence of the fear of crime; age of residents; religion of residents; relationships with the Police, and the levels of support being offered by other public sector agencies, such as local authorities, government departments or national neighbourhood watch support groups.[912] It must be stated quite clearly that establishing accurate information on the number of active neighbourhood watch schemes in each country of the UK is a very difficult exercise to undertake, due to two principal reasons. Firstly, there is no single reliable source of accurate information on the number of neighbourhood watch schemes in the UK. Secondly, information on numbers of schemes which is supplied from the national co-ordinating bodies for neighbourhood watch in the UK, i.e. Neighbourhood Watch Scotland; the Neighbourhood and Home Watch Network for England and Wales, and the Northern Ireland Policing Board (as representing the 3 Northern Ireland co-ordinating bodies), includes only those schemes which have been registered with these bodies, or the information has been supplied from studies which have been undertaken. However, there is evidence of the existence of a substantial and admittedly unquantifiable number of other 'live' schemes which have not been registered with the national co-ordinating bodies, but nevertheless have the same status, role and characteristics of schemes which are 'registered'. Schemes which have registered with the national co-ordinating bodies can receive information and guidance about starting up and fulfilling their role; advice on where to buy useful items such as signs and stickers, and can also register to receive national email alerts for dissemination on particular issues of safety relating to personal security, property, internet safety and for example keeping warm during the winter (see Section 2.2.1 concerning neighbourhood watch electronic alerts). It should be noted that schemes which have not been registered with the national co-ordinating bodies are not inferior to or have a lower status than schemes which have been registered. Schemes which are registered with the national co-ordinating bodies are more likely, than those which are not, to receive advice

[911] Nicholas, Siân, John Flatley (eds.) et al, Circumstances of Crime, Neighbourhood Watch Membership and Perceptions of Policing: Supplementary Volume 3 to Crime in England and Wales 2006/07: Findings from the 2006/07 British Crime Survey, Home Office, 2008.
[912] McConville, Mike, Dan Shepherd, Watching police, watching communities, Routledge, 2013.

and assistance from the local police about their how to operate their neighbourhood watch scheme, and how to interact with the police. Laycock and Tilley provide evidence of the high number of schemes which were in existence in 1995:

'The growth of Neighbourhood Watch has been a crime prevention success story. There are now over 130,000 schemes in the United Kingdom all testifying to the commitment felt by the public to working with the police and other groups in controlling crime.'[913]

Further information regarding the numbers of schemes and their spatial distribution amongst the four home nations of the UK is provided in the following chapters, including information concerning the national characteristics of neighbourhood watch activities in each of the four countries, and some reasoning as to why schemes are not registered with national co-ordinating bodies.

2.2.1 Scotland

According to the website of Neighbourhood Watch Scotland, the national co-ordinating body, neighbourhood watch started in Scotland in the early 1980s, and the latest information on numbers of schemes shows: 'Currently there are around 1600 registered schemes in Scotland, covering over 90,000 households. This number is growing steadily as new watches are established'.[914] National co-ordination of neighbourhood watch activities in Scotland commenced in 2006 with the Association of Scottish Neighbourhood watches, which subsequently changed its name to Neighbourhood Watch Scotland in 2011, and is registered as a Scottish Charitable Incorporated Organisation. It employs 2 members of staff and is governed by a Board of Volunteer Trustees, with funding being provided by the

[913] Laycock, Gloria and Nick Tilley, Policing and Neighbourhood Watch: Strategic Issues, Home Office Police Research Group, 1995, p.12.
[914] Neighbourhood Watch Scotland: http://www.neighbourhoodwatchscotland.co.uk/pages/1363/1/What_is_Neighbourhood_Watch_Scotland_.html

Scottish Government. One of its key objectives is stated as: 'Our aim is to help people work together to make their communities safer.'[915] As stated previously, it is very difficult to obtain reliable information on the numbers of schemes which are active, and there is evidence of fluctuating changes in the number of active schemes, both downwards and upwards, over periods of time. This fact is exemplified by Fyfe[916] who records that in 1996/97 within the Strathclyde Police force area alone, there were 1,671 schemes, and 4,597 within Scotland, although by 2005/06, there were 427 schemes within Strathclyde and 2,874 within Scotland.[917] Fyfe ascribes the growth in interest in neighbourhood watch to government policies in the 1990s which promoted active citizenship, and 'civilian policing' which took the form primarily of neighbourhood watch and special constables.[918] The Association of Chief Police Officers in Scotland (ACPOS) also acknowledges the work of special constables and community wardens in assisting community police officers: 'The targeted use of the Special Constabulary, volunteers and community wardens will provide resilience and support the work undertaken by community police officers.'[919] Fyfe, however, attributes the reasons why there was such a fall in the numbers of neighbourhood watch schemes across Scotland between 1996/97 and 2005/06, thus:

'These temporal trends are important, perhaps suggesting that public enthusiasm for this type of civilian policing is diminishing as recognition grows that Neighbourhood Watch has little impact on reducing levels of victimisation……..'[920]

---

[915] Ibid
[916] Fyfe, Nicholas R., Policing Crime and Disorder, in Policing Scotland, Daniel Donnelly and Kenneth Scott (eds.), Wilan, 2013, p.190.
[917] The Strathclyde Police Force was the largest of Scotland's 8 regional forces, which was amalgamated (along with the former Scottish Crime and Drug Enforcement Agency) as a single police force, Police Scotland, on 1 April, 2013: http://www.scotland.police.uk/about-us/
[918] Special Constables are civilians who carry out regular policing duties on a part-time and unpaid basis. The extent of their training will determine the range of duties which they execute.
[919] ACPOS Public Reassurance Strategy: http://www.sipr.ac.uk/downloads/ACPOS_Public_Reassurance_Strategy_310707.pdf
[920] Fyfe, Nicholas R., Policing Crime and Disorder, in Policing Scotland, Daniel Donnelly and Kenneth Scott (eds.), Wilan, 2013, p.190.

A major achievement of Neighbourhood Watch Scotland has been the successful establishment in 2010 of a single database of neighbourhood watch schemes in Scotland, which Neighbourhood Watch Scotland administers, following close working with Scotland's then 8 police forces.[921] The spatial distribution of neighbourhood watch schemes in Scotland covers the entire country, and includes homes in both rural and urban areas, although there are vast geographical parts of Scotland which have no coverage at all, typically sparsely populated areas, such as the highlands and islands. The average number of members in each scheme (in Scotland) is thought to be around 20. There is some evidence (gained from the empirical work carried out in IRISS WP4 on crime prevention, in particular, Interview CP 3), which points to the likelihood of a much higher number of schemes in existence than those recorded by Neighbourhood Watch Scotland. The reasons for schemes not being registered is thought by Interviewee CP 3 to include:

'*The system does have its faults as neighbourhood watch schemes are not always registered with Neighbourhood Watch Scotland. This is possibly due to the loss of independence about taking control of their own activities. The number of schemes is quite high which are not registered with Neighbourhood Watch Scotland in our region'.*'[922]

In recent years there has been a discernible change from neighbourhood watch activities being centred on 'soft' surveillance and the monitoring and reporting of suspicious activity and movements, to a more inclusive and caring approach in which improving the safety of communities features strongly and involves for example, giving advice about online security, bogus caller alert schemes, semi-formal arrangements for sharing of holiday information with neighbours, and generally making vulnerable people feel safer. An example of this move towards

[921] Police Scotland was formed as Scotland's single police force on 1 April, 2013 replacing the former 8 regional police forces and the Scottish Crime and Drug Enforcement Agency: http://www.scotland.police.uk/about-us/

[922] Interview, IRISS Project: irissproject.eu/: Crime Prevention Interview No. 3 (STIR).

a more humanitarian role can be found on the Neighbourhood Watch Scotland website[923] which offers the following examples of how to care for neighbours and family members:

'In previous years, severe weather left some people vulnerable. Helping each other a little can make a big difference. Here's how you can play your part in making your community more prepared:
Identify family members or neighbours who may need an extra helping hand if severe weather strikes
Have their phone numbers to hand
Offer to help with grocery shopping or other essential tasks
Clear ice or snow from pathways
Volunteer to help others by visiting www.volunteerscotland.org.uk
If you are part of a community group, think about what your group can do to help others during bad weather'

Neighbourhood Watch Scotland has also introduced an 'alert' messaging system where people or schemes who have registered with them receive email alerts on issues which are currently urgent or topical. Taking the latest 10 alerts,[924] these provide good examples of this changing focus of neighbourhood watch away from purely reporting property or neighbourhood crime, towards a more caring and supporting role, with a strong emphasis too on awareness of internet safety:

Keeping safe and warm this winter – 25.11.13
Mass e-mail spam attack warning – 19.11.13
UK faces mass 'ransomware' email attack from cybercriminal gangs – 19.11.13

[923] Neighbourhood Watch Scotland: http://www.neighbourhoodwatchscotland.co.uk/da/55735/Are_you_Ready_for_Winter_.html
[924] Neighbourhood Watch Scotland. Accessed, 25.11.13: http://www.neighbourhoodwatchscotland.co.uk/alert_archive

Stay safe from scams – 14.11.13

Cold Callers, Kirkliston – 13.11.13

SACRO's "Love Thy Neighbour" Competition – 12.11.13

Bogus Gardener, Drylaw & Craigleith – 11.11.13

Have your say on Edinburgh's safety priorities – 8.11.13

Gardening scam, Drylaw – 6.11.13

Royal Cornhill Hospital fire - 5th of November – 6.11.13

Key partners of Neighbourhood Watch Scotland are shown in ANNEX I. Neighbourhood Watch Scotland also encourages other forms of 'watch' activities which are closely linked to many other initiatives which promote and support personal and community safety, such as Community Speedwatch (targeting roads which are deemed to have problems with speeding motorists); Shopwatch (where information on known offenders such as shoplifters is shared); Horsewatch; Farm Watch, and Pubwatch (where information on known troublemakers, including sometimes their photographs, is shared amongst licensed premises). The legitimacy aspects of these other 'watch' schemes have not been explored in relation to sharing of information and the implications which this has for data protection, privacy and human rights.

2.2.2 England and Wales

Neighbourhood Watch in the UK was originally called Home Watch, a name by which it is still known in some parts of England and Wales. In 2007, with support from the Home Office, the Neighbourhood and Home Watch Network (England & Wales) was formed.[925] Prior to this, there had been a national co-ordinating body for England and Wales called the UK Neighbourhood Watch Trust, however this was disbanded due to internal and irreconcilable

[925] Neighbourhood and Home Watch Network (England and Wales): http://www.ourwatch.org.uk/about_us/our_history/

differences amongst some of the members and co-ordinators, which may explain why some current members and co-ordinators of neighbourhood watch schemes are unwilling to register with the national database, or to become involved with national initiatives. For example, in Wales there is some active opposition by their members and coordinators to the national database, and as a result, fewer schemes have registered than are known to exist. The Neighbourhood and Home Watch Network currently have seven employees, and provide support to new groups wishing to start-up, including directing people towards the various resources on their website, such as Toolkits, a Document Library, and a Members Area.[926] Local Associations may provide further and more detailed support depending on the characteristics of the area, what the local issues are, and what the relationships are like between the local Neighbourhood Watch groups and the police.

The coverage of neighbourhood watch in the UK for 2006/07 is recorded by the British Crime Survey as '…… 16 per cent of households currently belong to a Neighbourhood Watch scheme (this equates to an estimated 3.8m member households in England and Wales).'[927] However, the Neighbourhood and Home Watch Network believe that the number of schemes registered with them may 'just be the tip of the iceberg of how many schemes exist.' Their national database of schemes has only been operational for around 3 years, and relies on self-registration of schemes by co-ordinators. At 1 November, 2013, there were 12,324 registered schemes, and over 190,000 registered 'users' on their database, many of whom are believed to be co-ordinators who have not registered their scheme online or who do not have the technical ability to do so.[928] The Network believes that neighbourhood watch members tend to be older members of the community. The Network can analyse their membership, coordinators and 'users' by certain demographic groupings

[926] Neighbourhood and Home Watch Network: http:// www.ourwatch.org.uk
[927] Nicholas, Siân, John Flatley (eds.) et al, Circumstances of Crime, Neighbourhood Watch Membership and Perceptions of Policing: Supplementary Volume 3 to Crime in England and Wales 2006/07: Findings from the 2006/07 British Crime Survey, Home Office, 2008
[928] Neighbourhood and Home Watch Network, email correspondence with STIR, dated 20.11.13 and 21.11.13.

(e.g. age, ethnicity, disability, religion etc.), but they do not have the permissions necessary to determine socio-economic or other types of groupings on a neighbourhood basis. In some areas however, the local police force has purchased a licence to use the Network's database, e.g. Leicestershire, Lincolnshire, Nottinghamshire, Northamptonshire, Derbyshire, Cambridgeshire, Cumbria and Cheshire.[929] In England and Wales, a major change was introduced recently in the way that priorities are decided for policing within the 41 policing areas: 'On 15 September 2011 the Police Reform & Social Responsibility Act received Royal Assent, paving the way for the election of Police and Crime Commissioners (PCCs) for 41 of the 43 police force areas across England and Wales.'[930] This change introduced autonomous Police and Crime Commissioners who have direct responsibility for the following:

being directly accountable to the scrutiny of the public;
having the democratic mandate to respond to local people's concerns;
setting local force's policing priorities and force budget;
working with local partners to prevent crime;
holding their Chief Constable to account for the performance of the force,
appointing, and where necessary dismissing, the Chief Constable[931]

The Neighbourhood and Home Watch Network are also active in the field of research, including having undertaken a Loneliness and Isolation survey in 2013[932] which showed that neighbourhood watch members were less likely than non-members to feel isolated or lonely. The Network are also analysing the results of a survey on 'Perceptions of Crime' which

[929] Ibid.
[930] Gov.uk: https://www.gov.uk/police-and-crime-commissioners
[931] Police.uk: http://www.police.uk/information-and-advice/police-and-crime-commissioners/
[932] Neighbourhood and Home Watch Network: http://www.ourwatch.org.uk/resource_centre/document_library/loneliness_isolation_survey_august_2013/

achieved over 15,000 responses, and work is due to start soon on a series of case studies into particular neighbourhood watch schemes and initiatives.

2.2.3 Northern Ireland

NI Direct, Government Services,[933] the website of the Northern Ireland Executive (which exercises executive authority on behalf of the Northern Ireland Assembly), provides useful information on neighbourhood watch in Northern Ireland, including what it can do, how to become involved, how to start up new schemes etc. The Northern Ireland Policing Board[934] have advised that as of November, 2013 there are 776 registered neighbourhood watch schemes, with 1,336 co-ordinators, covering 52,823 households. Local co-ordination of neighbourhood watch is carried out by the Neighbourhood Policing Teams, and the Police and Community Safety Partnerships. Overall co-ordination of neighbourhood watch in Northern Ireland is undertaken by a steering group involving representatives of three organisations, whose details and purpose are described as follows:

'*The aim of Neighbourhood Watch is to support you so that you can protect yourself and your property. The scheme is promoted, supported and endorsed at a strategic level by a partnership (Steering Group) comprising representatives of the Department of Justice,*[935] *the Police Service of Northern Ireland (PSNI)* [936] *and the Northern Ireland Policing Board (NIPB). At an operational level, this is done through PSNI District Command Units and Policing and Community Safety Partnerships.*'[937]

[933] NIDirect, Northern Ireland Government's website: http://www.nidirect.gov.uk/neighbourhood-watch
[934] Northern Ireland Policing Board: http://www.nipolicingboard.org.uk/

[935] Department of Justice, Northern Ireland: http://www.dojni.gov.uk/
[936] Police Service of Northern Ireland: http://www.psni.police.uk/
[937] NIDirect, Northern Ireland Government's website: http://www.nidirect.gov.uk/neighbourhood-watch

In 2012, a report, commissioned by the Department of Justice, the Northern Ireland Policing Board and the Police Service Northern Ireland, was published on 'The Evaluation of Neighbourhood Watch.' The aim of the research was to assess the views and experiences of residents on the impact and effectiveness of Neighbourhood Watch in relation to the following areas:

Reducing crime, the fear of crime and antisocial behaviour;

Assisting the local police in detecting crime;

Enhancing the relationship between the police and the community and other partner agencies;

Promoting community spirit, and

How Neighbourhood Watch in Northern Ireland should be developed.'[938]

The report was completed by Perceptive Insight[939] who recorded that there were 635 accredited schemes as of August 2011, covering 49,000 households. A further, and related, study was undertaken on the mapping of neighbourhood watch schemes in Northern Ireland. Topping[940] recorded that, at the time of writing (2012), 0.5% of neighbourhood watch schemes were located in COA's (census output areas)[941] which reside in the top 10% of the multiple deprivation measure (i.e. most deprived areas), while 90% reside in the bottom 10% of the multiple deprivation measure (i.e. least deprived areas). There was another significant socio-demographic factor which influenced the membership of neighbourhood watch schemes in Northern Ireland, and that was religion, with the vast majority of members being of protestant as opposed to catholic faith. This religious demographic feature of neighbourhood watch schemes in Northern Ireland is thought to be particular only to

[938] Perceptive Insight, Evaluation of Neighbourhood Watch, Final Report, July, 2012, p.2.
[939] Ibid, p.9
[940] Topping, John, Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake, p.6, 2012.
[941] Census Output area is defined as an area with populations of approximately 340 people. There were 5052 COA's in N. Ireland in 2012.

Northern Ireland, and not to the other countries of the UK. Although neighbourhood watch is recorded as being a relatively recent phenomenon in Northern Ireland (commencing in 2004), neighbourhood watch was known to be in existence prior to this, and may have been called the Good Neighbour Scheme or Home Watch. The Northern Ireland Peace Agreement[942] which was concluded in 1998, set the ground for peaceful civil relations to be established between the unionist and nationalist communities, and there has been sustained growth in the numbers and coverage of schemes in the last decade. What appears to be a main difference between the schemes in Northern Ireland and the rest of the UK is the more prominent and active role which the Police continue to undertake, in establishing and supporting neighbourhood watch schemes, with a strong emphasis placed on 'neighbourhood safety; reducing the fear of crime; anti-social behaviour, and protecting yourself and your property.'[943]

3. Stakeholders and Partners

Since its introduction, neighbourhood watch in the UK has been supported to varying degrees and at different times by major stakeholders (and partners) such as the UK and Scottish Governments, the Northern Ireland Assembly, politicians, the Police, local community safety partnerships, and by local authorities, often on the back of various campaigns and initiatives which have been promoted at different times, such as community policing, community safety, community planning, and the introduction of community wardens. This support has taken different forms, such as working with partners in a (community planning) multi-agency approach to tackling social problems, to deployment of community police officers, increasing the number of police patrols in response to community

[942] Gilbert, Geoff; Colin Warbrick, Dominic McGoldrick, The Northern Ireland Peace Agreement, Minority Rights and Self-Determination, The International and Comparative Law Quarterly, 1998, 47, 4, 943-950.
[943] Northern Ireland Policing Board, Policing and Community Safety Partnerships, Neighbourhood Watch: http://www.nipolicingboard.org.uk/index/our-work/policing_and_community_safety_partnerships/neighbourhoodwatch.htm

concerns, and the use of community wardens to actively facilitate the establishment of new Neighbourhood Watch schemes. Other stakeholders in neighbourhood watch include not least the communities which the schemes serve. The network of partner organisations is now quite extensive with which neighbourhood watch schemes interact in the public, private and third sectors, and fuller details are shown in ANNEX I for Scotland, and ANNEX II for England and Wales. Interestingly, at the local level, the changing focus of neighbourhood watch activities, as described in more detail earlier in the case study, towards a more caring approach for individuals in a community, as opposed to monitoring criminal activities, has also witnessed an extension of the links which neighbourhood watch schemes now have with organisations particularly in the private and third sectors who are involved in the provision of services or equipment which can assist neighbourhood watch schemes in meeting their increasing involvement in issues of social responsibility.

4. Online Media and Communication

Both Neighbourhood Watch Scotland and the Neighbourhood and Home Watch Network use the same powerful online tool 'Neighbourhood Alert' to communicate electronic messages and newsletters to neighbourhood watch co-ordinators and registered 'users' within a precisely targeted geographical area, regionally or nationally. This common technology would make it easy for both organisations to share information if they choose to do so. In Scotland, this has the potential to reach around 1,600 schemes covering approximately 90,000 homes, and in England and Wales there are 12,324 schemes with over 190,000 'users.' However, there is thought to be a very large number of schemes which have not registered with the national co-ordinating bodies, and therefore miss out on these 'alerts'. There is also the disadvantage of not being able to communicate with those co-ordinators who have registered their schemes but have not registered their electronic contact details. Initially, prior to the introduction of the 'Neighbourhood Alert' system, the national co-ordinators in England and Wales relied heavily on their key contact persons in each of the 43

geographical areas of England and Wales for disseminating information, although this system was regarded as being inherently weak. In one rural region of Scotland, with 4 distinct geographical districts, a simple but very effective communication protocol has been developed which involves a telephone cascade system to pass on communications. There are 5 or 6 people in each contact group, which includes the principal contact person, to whom the message is passed, who then passes it to people below, who in turn pass it on again to others in the various neighbourhood watch schemes. The success of this initiative appears to be in its simplicity, and co-ordinators will receive calls back to confirm that the message has been conveyed and cascaded properly. The system is claimed to have the potential to pass a message on to almost 5,000 households within a very short time, if it all goes smoothly. The organiser of this cascade system states that: 'it ensures that lots of eyes and ears are looking and listening.'[944]

5. External Accountability and Regulation

Members of neighbourhood watch schemes are volunteers, they are not armed or uniformed, and are not usually subject to any formal checks (such as criminal records) on their suitability to give advice, conduct surveillance or carry out other monitoring activities in their designated locale. National co-ordinating bodies give advice on how to establish a scheme which includes provision of a draft constitution, although it is not known how many schemes actually adopt a constitution and then comply with its requirements. To that extent, neighbourhood watch schemes can be regarded as self-regulating. The fact that neighbourhood watch scheme members are unelected and volunteers, does call into question the legitimacy and representativeness of their 'voice', however there is undoubted widespread support for their activities, and participation in neighbourhood watch activities is

[944] Interview, IRISS Project: irissproject.eu/, Crime Prevention No. 3 (STIR).

a commendable form of active citizenship[945] and members should be recognised for the contribution which they make to the safety of their community. The average age of volunteers is thought to fall into the older persons' category (aged 50 and over). Financial support for neighbourhood watch in Scotland is provided by the Scottish Government in the form of a direct grant to Neighbourhood Watch Scotland, an independent charity, which allows the rental of premises and the employment of one full-time and one part-time member of staff who co-ordinate neighbourhood watch activities and disseminate guidance and information on a Scotland-wide basis. It would fair to say that a 'light touch' is employed with regard to regulation of neighbourhood watch activities by Neighbourhood Watch Scotland. Similarly, in England and Wales, the Home Office funds the Neighbourhood and Home Watch Network, which employs seven staff. In Northern Ireland, funding for neighbourhood watch support is provided through the Northern Ireland Assembly to the three organisations who co-ordinate neighbourhood watch in the province: the Department of Justice, the Northern Ireland Policing Board, and the Police Service Northern Ireland. The extent to which neighbourhood watch schemes and its members are accountable to their local community is hard to establish, although it is most likely that an annual meeting will be held which may be open to the public, and information on local safety issues will be communicated (most likely) to all households in the area, irrespective of whether or not they are members of the neighbourhood watch scheme.

6. Resilience and Controversies

There is evidence that community resilience in the form of neighbourhood watch activity and interest is stronger in areas which have higher levels of people with shared backgrounds in terms of (house) owner-occupancy, housing turnover rates, professional backgrounds, and employment, compared to fewer schemes in areas which have lower levels in each of these

[945] Fyfe, Nicholas R., Policing Crime and Disorder, in Policing Scotland, Daniel Donnelly and Kenneth Scott (eds.), Wilan, 2013.

categories.[946] What remains irrefutable, is the fact that neighbourhood watch, as a form of community resilience as a response to societal problems, to criminality or to the fear of crime, remains active across all parts of the UK, and that the extent of this resilience, although difficult to assess accurately, extends to hundreds of thousands of homes and potentially several million residents.

It would probably be inaccurate to say that there have been controversial moments in the development of neighbourhood watch in the UK, although this subject does require further research. It would probably be more accurate to say at this stage that the changing activities of neighbourhood watch can be seen to be in response to other changes occurring in society, and to changes occurring within organisations operating at a national level. If we take community policing for example, there was a huge drive for this initiative in Scotland (at a national level) a number of years ago and strong links were developed for example between communities, schools and neighbourhood watch groups and their community police officer. The community police officer was seen by many neighbourhood watch groups as their main point of contact and information transferred backwards and forwards between the two. However, due to national funding restrictions[947] and a subtle policy shift away from community policing, the Police are now mostly unable to sustain those same levels of community engagement as they did hitherto. This has led to more involvement in some cases by community wardens, such as dealing with anti-social behaviour, but for some neighbourhood watch groups, their focus has been subject to a noticeable change, involving them demonstrating their resilience by taking charge of their own affairs, often in caring ways such as passing on information about the threat of bogus callers, how to protect your home, and sharing information with each other (and in some cases with the Police) about holiday plans and keyholder information for when they will be absent from their home. In some cases neighbourhood watch groups have arisen as a direct response to householders' common experience of house breakings, which has had an added benefit of the neighbourhood watch members engaging with each other on a social basis more often than they

[946] Topping, John, Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake, p.6, 2012.
[947] BBC News, 2.10.13: http://www.bbc.co.uk/news/uk-scotland-24359112

did before, as evidenced in an interview conducted for the Crime Prevention topic for the IRISS project, WP4:

'This (forming a neighbourhood watch scheme) all helps us to get to know the neighbours much better, and we now let each other know when we will be away or on holiday. Things have now quietened down and there has been no trouble, but we are all much more alert.'[948]

7. The Changing Role of the Police

Since the inception of the first neighbourhood watch schemes in the UK in the early to mid-1980s, the role of the police has had a major influence on the growth, sustainability and diversity of interests of neighbourhood watch schemes. The police can rightly be attributed to having engendered resilience within communities by encouraging them to form neighbourhood watch schemes, and as previously outlined in Section 2.1, Police in the UK according to Bolton[949] were responsible for promoting neighbourhood watch as a form of active citizenship to reduce the costs of policing. Fyfe[950] and Henry[951] however, attribute successive governmental policies as being responsible for promoting the growth of neighbourhood watch as part of the drive to increase the development and reach of community policing. McConville and Shepherd also expand on the rhetorical support provided for neighbourhood watch by politicians, including those at governmental level.[952] The role of politicians and governments in directing the activities of the police is an important one, and undoubtedly has had a major influence on the relationship between the police and neighbourhood watch. The Scottish Government for example created 15 national outcomes, one of which is 'we live our lives safe from crime, disorder and danger',[953]

[948] Interview, IRISS Project: irissproject.eu/: Crime Prevention Interview No. 7 (STIR).
[949] Bolton, Sharon, Crime prevention in the community: The case of Neighbourhood Watch, Taylor & Francis,
2006, p.40.
[950] Fyfe, Nicholas R., Policing Crime and Disorder, in Policing Scotland, Daniel Donnelly and Kenneth Scott (eds.), Wilan, 2013.
[951] Henry, Alistair, The development of community safety in Scotland: a different path? Crime prevention policies in comparative perspective, Willan Publishing, 2009, pp.86-109.
[952] McConville, Mike, and Dan Shepherd, Watching police, watching communities, Routledge, 2013.
[953] Scottish Government, National Outcomes:
http://www.scotland.gov.uk/About/Performance/scotPerforms/outcomes

and one of the 5 national strategic objectives is to make Scotland 'safer and stronger'[954] with an emphasis on community safety. Part of the approach in Scotland to resolving problems of crime and fear of crime (along with many other societal problems such as youth unemployment, and anti-social behaviour), has been to use partnership working, legislative provision for which has been made through the creation of community plans, involving all of the public sector organisations, including the police, within a community plan area working together to solve these types of problems, which are often inter-related:

'In November 2007 national and local government signed a concordat which committed both to moving towards Single Outcome Agreements (SOAs) for all 32 of Scotland's councils and extending these to Community Planning Partnerships (CPPs). The Scottish Government and local government share an ambition to see Scotland's public services working together with private and voluntary sector partners, to improve the quality of life and opportunities in life for people across Scotland.'[955]

Initially, and up until the last few years, the primary focus of neighbourhood watch in Scotland was on crime prevention, and the surveillance of activities and movements within geographically defined neighbourhoods, or streets, and the reporting of suspicious behaviour to the Police or other regulatory bodies, such as the local authority. During the 1980s and 1990s there was a strong drive towards community policing in Scotland,[956] including putting more police officers into communities, helping to establish links with local groups and schools, plus developing neighbourhood watch schemes. However, in recent years there has been a general reduction in these forms of community policing due to changing priorities of the Police which include having to save £1.7bn with the creation of Police Scotland, where the 8 former regional forces have been amalgamated into a single force. These changing priorities, which will see the closure of many police stations and reduced opening hours for

[954] The Scottish Government, national strategic objective – A safer and stronger Scotland: http://www.scotland.gov.uk/About/Performance/scotPerforms/objectives/safeAndStronger
[955] The Scottish Government: http://www.scotland.gov.uk/Topics/Government/PublicServiceReform/CP/SOA2012
[956] Henry, Alistair, The development of community safety in Scotland: a different path? Crime prevention policies in comparative perspective, Willan Publishing, 2009, pp.86-109.

others, will undoubtedly have an effect on community safety initiatives involving the police, with the likelihood of there being fewer police officers engaging with communities.[957] The changing focus of neighbourhood watch schemes in Scotland in recent years towards a more caring approach in terms of looking after neighbours, instead of reporting acts of criminality or unusual movements within an area, could be attributable, in part, to the changing role of community policing. A serving Police Officer of Police Scotland who was interviewed on the area of Crime Prevention for the IRISS project, WP4, gave his opinion on the changing roles of neighbourhood watch and the Police:

'Regarding Neighbourhood watch, there is no prescriptive advice which I give, although there has been a shift from crime to community safety, e.g. road safety, playground safety, scamming advice, how to deal with illicit calls, so it has a much broadened scope now.'[958]

Donnelly also refers to the increasing role which Community Wardens are now playing, many aspects of which were formerly fulfilled by Community Police Officers (CPO's):

'Although wardens in Scotland do not possess police powers, their aims and objectives are identical in many respects to those of CPOs. The list below is a selection of goals and objectives given by community wardens in their responses which coincide with those of CPOs:

***.....** facilitate neighbourhood watch schemes.'*[959]

In England and Wales, a major change was recently introduced in the way that priorities are decided for policing within the 41 policing areas,[960] which introduced autonomous Police and Crime Commissioners who have direct responsibility for the following:

---

[957] BBC News, 2.10.13: http://www.bbc.co.uk/news/uk-scotland-24359112
[958] Interview, IRISS Project: irissproject.eu/, Crime Prevention No. 4 (STIR).
[959] Donnelly, Daniel, Community Wardens in Scotland: Practitioners' Views, The Howard Journal of Criminal Justice, Wiley Online Library, 47, 4, 2008, pp.371-382.

being directly accountable to the scrutiny of the public;

having the democratic mandate to respond to local people's concerns;

setting local force's policing priorities and force budget;

working with local partners to prevent crime;

holding their Chief Constable to account for the performance of the force,

appointing, and where necessary dismissing, the Chief Constable[961]

The public turnout for the elections on 15.11.12 was 15.1%[962] but voter information on the candidates was apparently restricted to being available online only, which will have excluded many voters. It is too early to assess what the impact will be on neighbourhood watch activities in England and Wales with the appointment of these Commissioners, but there may well now be more scope for lobbying for police resources to be deployed to tackle local problems than there might have been previously, where national priorities may have held sway.

In Northern Ireland, since 1994 when the first neighbourhood watch schemes were introduced, the police there are continuing to take an active interest in establishing and sustaining neighbourhood watch as a key priority of community policing. Indeed, it is the local Neighbourhood Policing Teams and the Police and Community Partnerships who are tasked with co-ordinating neighbourhood watch on a local basis, although the overall responsibility within the province is a shared one amongst the Northern Ireland Policing Board, the Police Service Northern Ireland, and the Department of Justice. There is a strong emphasis placed on 'neighbourhood safety; reducing the fear of crime; anti-social behaviour, and protecting yourself

[960] Gov.uk: https://www.gov.uk/police-and-crime-commissioners
[961] Police.uk: http://www.police.uk/information-and-advice/police-and-crime-commissioners/
[962] The Electoral Commission: http://www.electoralcommission.org.uk/__data/assets/pdf_file/0003/154353/PCC-Elections-Report.pdf

and your property.'[963] The current main focus of neighbourhood watch in Northern Ireland, is quite similar to the original activities of neighbourhood watch in the rest of the UK from the early 1980s to the early 2000s, and therefore a conclusion may be drawn that the police do in fact have a major influence on the activities of neighbourhood watch, when they are actively involved with it.

Statistics relating to fear of crime, household crime and burglary reveals some interesting facts when they are then related to the likelihood or not of establishing neighbourhood watch schemes:

'The 2009/10 BCS shows that there continues to be a reduction in the proportion of people who think crime in their local area had increased locally' [964]

'The 2009/10 BCS found that the risk of being a victim of any household crime was higher in the most deprived areas compared with the least deprived areas in England. Trends in household crime in the most and least deprived areas in England have been broadly similar between 2001/02 and 2009/10, with the exception of trends in burglary. There has been a statistically significant reduction in levels of burglary in the most deprived areas since 2001/02 but no significant change in the least deprived areas.'[965]

Paradoxically, various studies have shown consistently, that neighbourhood watch is less likely to established in areas of higher crime (which tend to be more deprived), and more likely to be established in areas of lower crime (which tend to be least deprived). [966]

---

[963] Northern Ireland Policing Board, Policing and Community Safety Partnerships, Neighbourhood Watch: http://www.nipolicingboard.org.uk/index/our-work/policing_and_community_safety_partnerships/neighbourhoodwatch.htm

[964] Flatley, John, Chris Kershaw, Kevin Smith, Rupert Chaplin, Debbie Moon, Crime in England and Wales 2009/10: Findings from the British Crime Survey and police recorded crime, Home Office, London, 2010, p110.

[965] Ibid, p165.

[966] Topping, John, Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake, 2012.

8. Conclusions

Neighbourhood watch in the UK has been in existence from the early 1980s, and has experienced in that time quite widely fluctuating levels of active support by communities who have shown resilience to threats or perceived threats to their communities, their properties or themselves, by forming neighbourhood watch schemes as a societal response. Accurate information is difficult to obtain on the numbers of schemes which are active in the UK due to a number of reasons, which include in particular, an unquantifiable number of schemes in existence which have not registered with the respective national co-ordinating group (and cannot therefore be counted). Best estimates of the current numbers of registered schemes in the UK, provided by the national co-ordinating bodies, are 12,324 for England and Wales, 1,600 for Scotland, and 776 for Northern Ireland. The British Crime Survey estimated that, in 2006/07, 16% of the UK population was covered by a neighbourhood watch scheme (which equates to 3.8m households in England and Wales).[967] Clearly therefore, from the early 1980s to the present day, there is substantial evidence of community resilience on a grand scale throughout the UK, to perceived or actual societal problems, by forming neighbourhood watch schemes involving many hundreds of thousands of homes and several million residents. In the last few years, there has been a noticeable shift in the focus of neighbourhood watch activities from monitoring criminal activity and unusual movements in an area, and having close relationships with the police, to a much more person-centred approach involving looking after the welfare of neighbours, making residents aware of the dangers of bogus callers, sharing information when properties will be empty, and now increasingly, being aware of internet fraud. Human relationships in the foregoing contexts are undoubtedly influenced by the conditions of visible and invisible surveillance, and primarily these experiences will be positive and reassuring ones.

[967] Nicholas, Siân, John Flatley (eds.) et al, Circumstances of Crime, Neighbourhood Watch Membership and Perceptions of Policing: Supplementary Volume 3 to Crime in England and Wales 2006/07: Findings from the 2006/07 British Crime Survey, Home Office, 2008.

Neighbourhood watch members are volunteers, they are unelected, groups tend to number around an average figure of 20, they are not normally subject to criminal records checks, they are not uniformed, they tend to be aged over 50, and groups are most commonly formed in more affluent areas, and less commonly found in poorer areas, which may have a higher density of social-rented housing and mix of ethnic communities. Members are not thought to have undertaken any acts of vigilantism, although the Neighbourhood and Home Watch Network (for England and Wales) issued a statement in 2011, around the time of major rioting in some of the UK's cities, warning neighbourhood watch groups not to engage in any acts of vigilantism, and urging them instead, to forge stronger links with the police.[968] Neighbourhood watch schemes will commonly have a constitution, but they do lack democratic legitimacy in the strictest sense, as members are unelected. However, members of neighbourhood watch schemes should not be criticised for any apparent democratic deficit, but should be commended instead for their willingness to engage in active citizenship on behalf of their community.

The British Crime Survey 2009/10[969] reports that you are more likely to be a victim of crime if you live in one of the most deprived areas than if you live in one of the least deprived areas of England. Evidence from the Topping[970] shows that there are far higher numbers of neighbourhood watch schemes in the least deprived areas than in the most deprived areas. This is also the conclusion of the British Crime Survey in 2006/07: 'In general, the characteristics associated with lower levels of membership were those related to having a higher risk of crime.'[971] Bennett, in an earlier study also supports this view.[972] The relationship in recent years between crime figures and the establishment of neighbourhood

[968] Neighbourhood and Home Watch Network: https://www.neighbourhoodlink.co.uk/index.asp?display_history_alert=true&alerts_history_idx=2678&nav_idx=0&page_idx=1

[969] Flatley, John, Chris Kershaw, Kevin Smith, Rupert Chaplin, Debbie Moon, Crime in England and Wales 2009/10: Findings from the British Crime Survey and police recorded crime, Home Office, London, 2010.

[970] Topping, John, Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake, 2012.

[971] Nicholas, Siân, John Flatley (eds.) et al, Circumstances of Crime, Neighbourhood Watch Membership and Perceptions of Policing: Supplementary Volume 3 to Crime in England and Wales 2006/07: Findings from the 2006/07 British Crime Survey, Home Office, 2008, p57.

[972] Bennett, Trevor, Themes and variations in neighbourhood watch, Crime, Policing And Place: Essays In Environmental Criminology, Routledge, 1992, pp.172-186.

watch schemes therefore appears to show an inverse relationship between areas with higher crime figures corresponding to fewer neighbourhood watch schemes being established. From the early 1980s to the late 1990s, the police took quite an active role in promoting neighbourhood watch as did many politicians, which undoubtedly had an impact on the growth of schemes, however this support has generally been diminishing across England and Wales, and Scotland, due to other priorities and diminishing resources. However, this is by no means a black and white picture, as 41 of the 43 police regions in England and Wales (from 2012) now have autonomous Police and Crime Commissioners who can respond to local needs and concerns. The position in Northern Ireland, where neighbourhood watch has been more actively promoted from around 2004, quite clearly shows a high level of ongoing police support for the establishment of neighbourhood watch across the province, but the reasons for this may be more complicated due to the relatively recent establishment of a lasting political peace, and with the new Police Service Northern Ireland, which was established in 2002, maintaining its drive to develop stronger community safety links than perhaps could have been achieved prior to the Northern Ireland Peace Agreement.[973] Surveillance practices used by neighbourhood watch schemes are not normally negotiated, or publicised, and do not tend to use surveillance technologies, and the balance of the surveillance power relationship therefore tends to lie with the neighbourhood watch members. Increasingly though, new social media is being used for communication purposes, particularly the 'Neighbourhood Alert' system, by the national co-ordinating bodies, and in a communications sense there has truly been a transformative change from the disjointed arrangements which were used previously, although many schemes are not registered with the national co-ordinating bodies and therefore miss out on communications alerts, while others may miss out due to lack of either internet access or technical ability to use the internet. According to the Neighbourhood and Home Watch Network, 'Neighbourhood Alerts' often feature in news and other media. Neither national news media nor politicians have

[973] Gilbert, Geoff, Colin Warbrick, Dominic McGoldrick, The Northern Ireland Peace Agreement, Minority Rights and Self-Determination, The International and Comparative Law Quarterly, 1998, 47, 4, 943-950,

generally used neighbourhood watch in a sensationalist fashion, or to manipulate fears. Surveillance practices undertaken by neighbourhood watch volunteers do not tend to use surveillance technologies, but communication methods by national neighbourhood watch co-ordinating bodies and neighbourhood watch groups locally, use new social media technologies extensively.

The context of the case study has been constructed from that of citizen: citizen, and has been developed from the perspectives of the 'watchers'. It has not been possible to obtain information from the 'watched'.

STIR

18 December, 2013

ANNEX I:

Key Partners of Neighbourhood Watch Scotland

1. Business watch
2. Church watch
3. **Community Councils**
4. **Crime Prevention Panels**
5. **Community Safety Partnerships**
6. Dog watch
7. Flood watch
8. **Fire and Rescue Services**
9. **Local authorities**

10. Metal watch
11. No Cold Calling Zone Areas
12. **Other charities or community groups**
13. **Police Scotland**
14. Rail watch
15. Rural watch
16. School Watch
17. **Scottish Business Resilience Centre (formerly The Scottish Business Crime Centre)**
18. Tenants and Residents Associations
19. **Trading Standards**

ANNEX II

Key Partners of the Neighbourhood and Home Watch Network (England and Wales)

1 VISAV Ltd: 'The Neighbourhood Alert system

1. Police Forces in England and Wales and the Association of Chief Police Officers (ACPOS)
2. Fire and Rescue Service and the Chief Fire Officers Association
3. The College of Policing
4. Local Authorities and Community Safety Partnerships
5. The Office of Fair Trading – bogus callers, rogue traders and scams
6. Action Fraud – national fraud and internet crime reporting centre
7. Fraud Alert – Metropolitan Police web pages about scams and fraud to help prevent people becoming the victim of crime
8. Age UK – improving lives of older people

9. Crimestoppers – claims to be the UK's only independent crime fighting charity - anonymous online forms and telephone lines
10. Suzy Lamplugh Trust – advocates of personal safety
11. Master Locksmiths Association
12. Neighbourhood Watch Scotland
13. CNI Network and Street Angels – Christian nightlife Initiatives
14. Faith Matters and MAMA – reducing attacks on muslims and reducing inter/intra faith tensions
15. The Big Lunch – aims to have as many people to sit down at least once a year to have lunch with their neighbours
16. Safety Net Associates – crime and justice consultants
17. Sold Secure – testing and certification company for security products
18. Living Streets – advocates for pedestrian safety
19. Friends of the Elderly
20. Your Square Mile (mutual association)
21. Volunteering England
22. Locality – nationwide network for community organisations
23. Landlord Referencing – information service regarding tenants' historical records
24. Community Christmas – encouraging communities to ensure that no old person is alone on Christmas Day unless they want to be
25. Streetbank – a website for sharing and lending skills and items with neighbours

References

ACPOS Public Reassurance Strategy: http://www.sipr.ac.uk/downloads/ACPOS_Public_Reassurance_Strategy_310707.pdf

BBC News, 2.10.13: http://www.bbc.co.uk/news/uk-scotland-24359112

Bennett, Trevor, Themes and variations in neighbourhood watch, Crime, Policing And Place: Essays In Environmental Criminology, Routledge, 1992, pp.172-186.

Bennett, Trevor; Katy Holloway, David P. Farrington, Does neighborhood watch reduce crime? A systematic review and meta-analysis, Journal of Experimental Criminology, 2, 4, 2006, Springer, pp.437-458.

Bolton, Sharon, Crime prevention in the community: The case of Neighbourhood Watch, Taylor & Francis, 2006, p.40.

Department of Justice, Northern Ireland: http://www.dojni.gov.uk/

Donnelly, Daniel, Community Wardens in Scotland: Practitioners' Views, The Howard Journal of Criminal Justice, Wiley Online Library, 47, 4, 2008, pp.371-382.

Flatley, John, Chris Kershaw, Kevin Smith, Rupert Chaplin, Debbie Moon, Crime in England and Wales 2009/10: Findings from the British Crime Survey and police recorded crime, Home Office, London, 2010.

Fyfe, Nicholas R., Policing Crime and Disorder, in Policing Scotland, Daniel Donnelly and Kenneth Scott (eds.), Wilan, 2013, p.190.

Gilbert, Geoff; Colin Warbrick, Dominic McGoldrick, The Northern Ireland Peace Agreement, Minority Rights and Self-Determination, The International and Comparative Law Quarterly, 47, 4, 1998, pp.943-950.

Gov.uk: https://www.gov.uk/police-and-crime-commissioners

Henry, Alistair, The development of community safety in Scotland: a different path? Crime prevention policies in comparative perspective, Willan Publishing, 2009, pp.86-109.

King, Michael, Social crime prevention a la Thatcher, The Howard Journal of Criminal Justice, 28, 4, 1989, Wiley Online Library, pp. 291-312.

Laycock, Gloria and Nick Tilley, Policing and Neighbourhood Watch: Strategic Issues, Home Office Police Research Group, 1995, p.12.

Levine, Mark, Rethinking bystander non-intervention: Social categorization and the evidence of witnesses at the James Bulger murder trial, Human Relations, 52, 9, 1999, Sage Publications, pp.1133-1155.

McConville, Mike, and Dan Shepherd, Watching police, watching communities, Routledge, 2013.

Neighbourhood and Home Watch Network for England and Wales: http://www.ourwatch.org.uk/

Neighbourhood and Home Watch Network (England and Wales): http://www.ourwatch.org.uk/about_us/our_history/

Neighbourhood and Home Watch Network, email correspondence with STIR, dated 20.11.13 and 21.11.13.

Neighbourhood and Home Watch Network: https://www.neighbourhoodlink.co.uk/index.asp?display_history_alert=true&alerts_history_idx=2678&nav_idx=0&page_idx=1

Neighbourhood and Home Watch Network: http://www.ourwatch.org.uk/resource_centre/document_library/loneliness_isolation_survey_august_2013/

Neighbourhood Watch Scotland: http://www.neighbourhoodwatchscotland.co.uk/

Neighbourhood Watch Scotland: http://www.neighbourhoodwatchscotland.co.uk/pages/1363/1/What_is_Neighbourhood_Watch_Scotland_.html

Neighbourhood Watch Scotland: http://www.neighbourhoodwatchscotland.co.uk/da/55735/Are_you_Ready_for_Winter_.html

Neighbourhood Watch Scotland. Accessed, 25.11.13: http://www.neighbourhoodwatchscotland.co.uk/alert_archive

Nicholas, Siân, John Flatley (eds.) et al, Circumstances of Crime, Neighbourhood Watch Membership and Perceptions of Policing: Supplementary Volume 3 to Crime in England and Wales 2006/07: Findings from the 2006/07 British Crime Survey, Home Office, 2008.

NIDirect, Northern Ireland Government's website: http://www.nidirect.gov.uk/neighbourhood-watch.

Northern Ireland Policing Board: http://www.nipolicingboard.org.uk/

Northern Ireland Policing Board, Policing and Community Safety Partnerships, Neighbourhood Watch: http://www.nipolicingboard.org.uk/index/our-work/policing_and_community_safety_partnerships/neighbourhoodwatch.htm

Perceptive Insight, Evaluation of Neighbourhood Watch, Final Report, July, 2012.

Platt, John, Social traps, American Psychological Association, 28, 8, 1973, p.641.

Police.uk: http://www.police.uk/information-and-advice/police-and-crime-commissioners/

Police Service of Northern Ireland: http://www.psni.police.uk/

Shotland, R. Lance, Lynne I. Goodstein, The role of bystanders in crime control, J.Soc.Iss., 40, 1, 1984, Wiley Online Library, pp.9-26.

The Electoral Commission, http://www.electoralcommission.org.uk/__data/assets/pdf_file/0003/154353/PCC-Elections-Report.pdf

The Scottish Government: http://www.scotland.gov.uk/Topics/Government/PublicServiceReform/CP/SOA2012

The Scottish Government, National Outcomes: http://www.scotland.gov.uk/About/Performance/scotPerforms/outcomes

The Scottish Government, national strategic objective – A safer and stronger Scotland: http://www.scotland.gov.uk/About/Performance/scotPerforms/objectives/safeAndStronger

Tilley, Nick, The development of community policing in England: networks, knowledge and neighbourhoods, John Wiley & Sons, Ltd., Chichester, UK, 2008, p.98.

Titus, Richard M, Residential burglary and the community response, Springer, 97, 1984, pp.97-130.

Topping, John, Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake, p.6, 2012.

Yarwood, Richard and Bill Edwards, Voluntary action in rural areas: the case of neighbourhood watch, Journal of Rural Studies, 11, 4, 1995, Elsevier, pp. 447-459.