Project acronym:	IRISS
Project title:	Increasing Resilience in Surveillance Societies
Project number:	290492
Programme:	FP7-SSH-2011-2
Objective:	To investigate societal effects of different surveillance practices from a multi-disciplinary social science and legal perspective.
Contract type:	Small or medium-scale focused research project
Start date of project:	01 February 2012
Duration:	36 months

Deliverable D4.2:
Conduct the observation/ interviews
Doing privacy in everyday encounters with surveillance

Local reports on the results of the empirical studies conducted in different countries (Austria, Germany, Slovakia, Italy, UK)

Coordinator	IRKS ï Institute for the Sociology of Law and Criminology
Dissemination level:	PU
Deliverable type:	Report
Version:	1
Submission date:	31. July 2014
Submission date:	16. September 2014

Authors:

Chapters	Lead	Contributors
First draft of report structure	IRKS: Alexander Neumann, Regina Berglez	IRKS: Reinhard Kreissl
Review of the report structure	IRISS WP 4 Workshop in February 2014	All involved partners
Chapter 1: Introduction/Methodology	IRKS: Reinhard Kreissl	IRKS: Regina Berglez Alexander Neumann, 1.5 (Country Reports: all partners)
Chapter 2: Privacy and Convenience	UH: Nils Zurawski	UniBW: Daniel Fischer, Wolfgang Bonß
Chapter 3: Privacy and Security	UCSC: Chiara Fonio	IRKS Reinhard Kreissl COMENIUS: Martin Kovaniļ
Chapter 4: Privacy and Sociality	OU: Keith Spiller	IRKS: Alexander Neumann, Regina Berglez
Chapter 5: Privacy and Trust & Fairness	IRKS: Reinhard Kreissl	STIR: Charles Leleux IRKS: Alexander Neumann
Chapter 6: Engagement and Security	STIR: William Webster	STIR: Charles Leleux
Chapter 7: Summary	IRKS: Reinhard Kreissl	
Annex I: Country Reports	IRKS: Reinhard Kreissl	All partners involved
Annex II: Interview Data	IRKS: Reinhard Kreissl	IRKS: Regina Berglez, Alexander Neumann
Annex III: Focus Group Handbock	ÖAW-ITA: Walter Peissl	
Annex VI: Focus Groups (task 4.3): Surveillance and Control	ÖAW-ITA: Walter Peissl	UniBW: Daniel Fischer, UH: Nils Zurawski UCSC: Chiara Fonio, Alessia Ceresa COMENIUS:Erik Láštic, Martin Kovaniļ, STIR: Charles Leleux OU: Keith Spiller

Contents

ABSTRACT

The main idea of IRISS WP 4 was to analyse surveillance as an element of everyday life of citizens. The starting point was a broad understanding of surveillance, reaching beyond the narrowly defined and targeted (nonetheless encompassing) surveillance practices of state authorities, justified with the need to combat and prevent crime and terrorism. We were interested in the mundane effects of surveillance practices emerging in the sectors of electronic commerce, telecommunication, social media and other areas. The basic assumption of WP 4 was that being a citizen in modern surveillance societies amounts to being transformed into a techno-social hybrid, i.e. a human being inexorably linked with data producing technologies, becoming a data-leaking container. While this ñontological shiftò is not necessarily reflected in citizensô understanding of who they are, it nonetheless affects their daily lives in many different ways. Citizens may entertain ideas of privacy, autonomy and selfhood rooted in pre-electronic times while at the same time acting under a regime of ñmundane governanceò. We started to enquire about the use of modern technologies and in the course of the interviews focussed on issues of surveillance in a more explicit manner. Over 200 qualitative interviews were conducted in a way that produced narratives (stories) of individual experiences with different kinds of technologies and/or surveillance practices. These stories then were analysed against the background of theoretical hypotheses of what it means in objective terms to live in a surveillance society. We assume that privacy no longer is the default state of mundane living, but has to be actively created. We captured this with the term privacy labour. Furthermore we construed a number of dilemmas or trade-off situations to guide our analysis. These dilemmas address the issue of privacy as a state or ñgoodò which is traded in for convenience (in electronic commerce), security (in law enforcement surveillance contexts), sociality (when using social media), mutual trust (in social relations at the workplace as well as in the relationship between citizens and the state), and engagement (in horizontal, neighbourhood watch-type surveillance relations). For each of these dilemmas we identified a number of stories demonstrating how our respondents as ñheroesò in the narrative solved the problems they encountered, strived for the goals they were pursuing or simply handled a dilemmatic situation. This created a comprehensive and multi-dimensional account of the effects of surveillance in everyday life.
Each of the main chapters does focus on one of these different dilemmas.

1 INTRODUCTION AND OVERALL FRAMEWORK FOR WP4

Reinhard Kreissl

What makes the IRISS project different from many other FP7 consortia investigating citizensô view of surveillance is the theoretical and methodological approach. The overall idea informing the work in IRISS is a dual perspective on the topics under investigation. Surveillance, privacy, data protection and resilience can be analysed from the perspective of an outside, detached observer. When taking this perspective, a concept like privacy is put into a larger theoretical and disciplinary context, normative questions of adequate and reasonable solutions for given problems are addressed and meticulously analysed. The analysis strives for logical clarity of definitions and generalized arguments for or against solutions to problems defined in a more or less abstract way (this strategy is pursued primarily in WP 1, 2 and 6).

As opposed to the external observerôs point of view the participantsô perspective looks at the phenomena under investigation so to speak from the inside, through the eyes of the actors involved. This perspective from within pursues a reconstructive strategy, trying to understand *how* citizens conceive of surveillance; *how* they organize their daily lives vis-à-vis mundane everyday problems while living in what can be termed from the observerôs perspective a ñsurveillance societyò. Here a different kind of logic may be in operation. Citizens may have an idiosyncratic view on issues like data protection, privacy and surveillance. They may entertain strong normative biases towards crime fight and surveillance; they may consider data protection as completely irrelevant or extremely important. All this has to be taken at face value and then integrated in a larger theoretical frame of interpretation. While there may be informed and uninformed citizens, they all have to handle their techno-social way of existence in a surveillance society individually. These different strategies of coping with surveillance can be reconstructed when taking the position of the participantsô perspective. This is what WP 4 is aiming for.

The difference of observer and participant perspective has been elaborated by Jürgen Habermas in his Theory of communicative action to account for two different ways of analysing social phenomena.[1] Habermas introduces the two complementary concepts of *system* and *life world* linked to the two complementary perspectives of analysis: taking an observerôs perspective fosters a type of analysis conceiving of society as a more or less robust system to which individual actors have to adapt, whilst from the participants perspective society emerges as a context of social interaction sustained and continuously reproduced by individual social actors. Both perspectives taken together produce a complex account of modern society. A similar analytical difference has been used by Anthony Giddens in his theory of structuration, analysing the interplay between agency and structure.[2]

In the context of WP 4 we are mainly drawing on the methodological aspects of this double perspective by focussing on the participantsô perspective in the way citizens describe their everyday use of modern (surveillance) technologies. Using the dual perspective of system and life world these technologies can be seen as systemic elements operating on the everyday or

[1] Habermas, Jürgen, *Theorie des kommunikativen Handelns* (Band 1 und 2), Frankfurt, Suhrkamp, 2011.
[2] Giddens, Anthony, *The Constitution of Society, Outline of the Theory of Structuration*, Cambridge, Polity Press 1984.

life world of the actors. They may be constraining the range of actions or extend the realm of communicative reach, their existence may be perceived as problematic by citizens or not. But although these technologies do have an effect on the life world of citizens, these effects are not deterministic. Being exposed to and using modern technologies always entails a creative or active element of appropriation and/or interpretation. At the same time technology has become a highly pervasive element of mundane life in Western society and this changes the lives of citizens in manifold and fundamental ways.
In WP 4 we chose a strategic approach to better understand how citizens organize their daily lives in a surveillance society, and if and how they develop resilient reactions. We start from the assumption that modern information and communication technology, as the basis for all kinds of surveillance activities, has a number of effects. These effects can be overt or covert. They can affect citizensô lives in a more or less subtle way. Many surveillance effects (such as e.g. social sorting in data bases) go largely unnoticed. Others, such as e.g. access controls at airports, are obvious, visible, and citizens are aware of their being subject to surveillance and control measures.

WP 4 takes its starting point from the everyday experience of European citizens, trying to understand how the pervasive use of modern technology shapes their lives and how they perceive their status as being surveilled data subjects (or techno-social hybrids).

In this introductory chapter we will first elaborate the methodological approach followed in our data gathering and analysis and then lay out some of the theoretical ideas informing this analysis. The chapter ends with a brief description of our sample and the findings of the country reports on surveillance conducted in this work package in five countries: Austria, Germany, Italy, Slovakia and the UK.

1.1 METHODOLOGICAL REMARKS ON INTERVIEWS IN WP4

The qualitative approach

In order to go beyond the level of findings produced by survey research on citizensô attitudes towards surveillance and also to better understand what resilience could mean in real world settings, we developed a specific approach to conduct interviews and analyse and interpret the data obtained. While survey research typically confronts respondents with a set of clear-cut alternatives and provides a specific cognitive frame by asking explicit questions, the approach we chose avoids this. In WP 4 we used a very general stimulus to start the interviews with our respondents by asking them about their use of IC-technology (from mobile phones and laptops to credit- and loyalty cards) and the different ways they were applying this technology (from peer-to-peer communication to online shopping to searching for information via search engines). We avoided the term ñsurveillanceò as an explicit stimulus to give our respondents the opportunity to develop their personal understanding, and also to find out whether they had second (critical) thoughts about the use of these technologies. In later stages of the interview respondents were asked whether they had any thoughts about the effects of technology use and whether they had thought about what happened to the data they were leaking while using the various technologies they had talked about, e.g. their mobile phone. In many cases this opened up the explicit problem of surveillance and provided an opportunity to elaborate on

the different dimensions of this topic. Again, we were not working along a list of questions to be asked, but left it to our respondents to bring up whatever they thought would be relevant. Nevertheless, a guiding code of practise was used by the interviewers to ensure that a few, main topics were at least raised in the course of the interview.

Interviews are always communicative events. Narrative interviews give the interviewers an active role in a dyadic situation. These interviews are not modelled after the standard quantitative survey methodology where it is assumed that all interfering influences should be eliminated to elicit an uncontaminated, unbiased ñtrueò response from the respondents to then be written down or recorded by the interviewer. Interviewers take the important role of the listener or audience. In a narrative setting it is the task of the respondent to tell a story in such a way that the interviewer can understand the overall plot. This includes an elaboration of desires, plans, strategies and goals, motivating the actions of the narrator. (And interviewers can ask for clarification and explication should one of these elements be missing in the account produced by the interviewee.)

Some remarks on the pros and cons of the chosen approach

Opting for such an open and qualitative approach to empirical research has a number of consequences. It helps to produce accounts of relatively high ecological validity. Respondents can use their own words and schema of relevance to talk about the use of technology. While interviews of this kind tend to display a certain internal narrative coherence, it can be difficult to compare statements and generalize across several individual cases. It is however, important to note that the type of findings and insights produced in the tradition of qualitative research methods are different from the knowledge produced by quantitative survey research. While survey research typically looks at the overall distribution of pre-defined characteristics in a population, qualitative data can be used to demonstrate how individuals understand, interpret or solve a (general) problem in a unique, but nonetheless instructive way. Giving respondents the floor to develop their views on a given topic produces a wide array of complex interpretations that should not be reduced post-hoc to a set of standard categories. Nonetheless a theoretical strategy to synthesise the findings is necessary to come to conclusions beyond the presentation of interesting but idiosyncratic single cases.

In our research we had a further problem to address since interviews were conducted in different countries and different languages, which poses issues of translation. Extended narratives have to be translated to make them accessible to the researchers in other countries. This makes a hermeneutic analysis, based on subtle differences in linguistic meaning extremely difficult.

Both points ï the thematic openness of the interviews and the problem of translation into a common language to make the data accessible to all involved researchers ï led us to adopt a more structural and theory-driven approach for the analysis of interviews. We chose the model of a story grammar to analyse our interviews (see below for more details).

The unit of analysis

Taking stories as the primary unit of analysis has an advantage when working across different cultures and languages. It is easier to ñtranslateò and compare stories/events between different cultural and linguistic settings than to identify attitudes or beliefs on the basis of translating whole interviews. When reconstructing beliefs and attitudes as stable mental constructs of

individuals on the basis of interview data one has to start from the linguistic surface structure. To understand an attitude or belief one has to consider subtle semantic differences. Indexical expressions as well as the complex meaning in spoken language can easily get lost when utterances of respondents in interviews are translated into a common, third language. Stories or events as larger grammatical units on the other hand, display a rather straightforward syntactic and semantic structure. When looking at narrative structures of stories it is not necessary to stick to a precise transcript of the spoken language, but rather to operate with a set of structural elements that are invariant across individual languages.

The role of the storyteller

The research strategy applied here could also be labelled ñ*event research*ò, i.e. it is not primarily the individual, her/his mental states and cultural attitudes we are looking at. The focus is on the individual as being actively involved in some sort of societal action (ñeventò) and the way s/he handles or understands this situation. We perceive the individuals we interviewed primarily as problem solvers, i.e. as persons acting in a given environment to achieve a goal or solve a problem. As mentioned above we used a simple stimulus to start the interviews by asking about the daily use of technology. When exposed to this question, subjects tend to respond with stories about their way of using mobile phones, computers, tablets, etc. Often our subjects produced stories where they took the position of the main actor, i.e. they acted or were acted upon in a situation and technology was in one way or another involved in the course of events. In the interviews we tried to elicit these kinds of stories (***ñ****What happened to you?****ò ñ****What did you do?*ò). So while there was no narrow focus on specific topics to be addressed, respondents were urged to use an active mode of narration to the extent possible, telling what they did, what happened to them and how they managed to solve a problem or make decision about the proper course of action.

Narrative interviews of this kind are not primarily aiming at *attitudes* or other constructs (what do respondents think, which decontextualized general beliefs do they hold about a certain object, etc.) but rather the focus is on the re-construction of events and situations (hereafter referred to as ñ*stories*ò) where our interviewees have been involved in one way or another. Focussing on these kinds of stories creates a different set of data, compared to classical questionnaire type research. Synthesizing typified constellations of attitudes and beliefs along the line of standard methodology may nonetheless occur at a later stage.

Stories elicited in interviews describe events. A good story is one, where a person can take one of three pragmatic roles as *hero*, *narrator* or *listener*.[3] Typically the interviewer takes the role of the listener whereas the interviewees act as narrator and often also as the hero of the story.

Being involved in an event, respondents as storytellers can take each of these different roles: they can present events (or ñchanges in states of the worldò) from a third personôs perspective. An example from our interviews would be:

[3] Lyotard, Jean-Francois, *The post-modern condition. A report on knowledge.* Manchester University Press, 1979:20 passim.

> *ñWhen you think about all these video cameras mounted on public buildings, you wonder how this affects individual rights é ò*

Here the respondent reports a situation where s/he was not immediately involved, but holds a position to the issue at hand. Following up on a statement like this we usually asked for personal experience to probably elicit a more personal story of the respondent in the role of the subject being captured on video, putting him in the position of the *hero*.

The perspective of the storyteller

With regard to the topics addressed in IRISS two other principal perspectives have to be envisaged: when discussing the problems of surveillance in the later stages of the interview, stories can be told from the perspective of the *watcher* or the *watched*. A surveillant relation is typically comprised of these two roles and depending at which end of this relation the hero stands, the stories will be different.
An example from a story told from the perspective of the watched could read like this:

> *ñThe boss of this company set up video cameras to control access to the premises but what he actually did was controlling the workers é ò*

In this sequence the respondent who worked in this company for some time is in the position of the *watched* and elaborates on the consequences and the lack of counter strategies (the ñbossò was the local tycoon and only employer in a small village and no one dared to approach him or criticise him for putting up the video cameras, though everybody was against it.)

Stories from the perspective of the *watchers* occur in our sample as well though not as often as stories from the perspective of the watched. How such a story from the watcherôs perspective looks, can be demonstrated in an interview with a young man working in a winter resort at a ski lift in Austria, controlling the tickets of the skiers, who have to produce a machine-readable ticket (swipe card) with a digitalized photo to pass through the barrier. The photo stored on the ticket appears on the screen in the control room and our respondent in principle had the opportunity to check the identity of the person using this ticket. He was elaborating on this situation and why and how one should stop certain individuals using another personôs ticket or not. (i.e. when the person presenting the swipe card ticket is not identical with the digital photo stored on the ticket presented). Such stories from the watcherôs perspective create completely different social dynamics as compared to stories told from the position of the watched.

Focussing on events/stories elicited in the interviews yields a number of complex accounts. These accounts demonstrate a wide array of different ways to handle surveillance (as watcher or watched). The interviews produce different scenarios, presenting the respondents in different roles as watchers and watched, in public space and private relations, as active agents or passive victims.

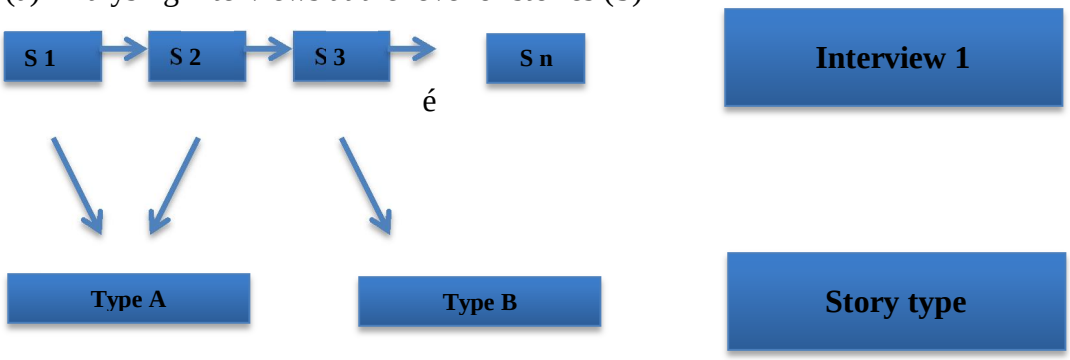
The (re-)actions of the storyteller

The types of interviews conducted in WP 4 primarily demonstrate how respondents solve the problems they encounter. Human behaviour (as presented in narratives about events and actions) can be understood as goal seeking or problem solving activity, or more generally as ñ*motivated*ò. People do things for a reason and when they are telling stories these reasons either have to be made explicit or they can be inferred using cultural knowledge (ñwhat every school child should knowé ò). As competent members of a culture we assume that individuals have intentions, follow plans, adopt strategies, that they can cheat, can address a problem straightforward etc. It is part of the cultural competence of members of society to read and comprehend the actions of the *heroes* in the stories they tell (or are told) in such a way that they infer plans or ascribe motives to the actors involved.

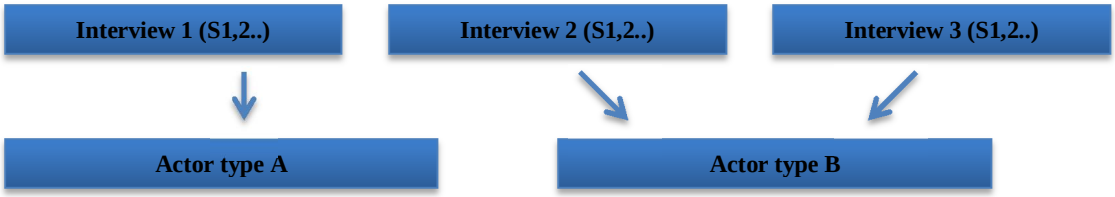
Taking this perspective opens up a number of options for the analysis of interview data. We can investigate how respondents ñsolveò or handle the problems they encounter. Hence we take interconnected *events* as presented in the format of a story as the basic unit of analysis. Identifying such stories/events is the first analytical step in the processing of the data obtained from our interviews.
Story or *event* are more complex units than attitudes and beliefs and most probably allow for a greater ecological validity of the field under investigation than abstract concepts.
Collecting individual stories from the interviews, one can work towards a typology of such stories. Having constructed such a typology of stories a second orthogonal step would be to develop a typology of actors. The chart below shows the logic of these different approaches to analyse the data.

Data analysis

(a) Analysing interviews at the level of stories (S)



(b) Comparing interviews to identify types of actors



Stories, as understood here, are cognitive cultural schemata used to summarize and process information about the world. Imagine a novel like Tolstoyôs *War and Peace*. A person having read this book is asked to give a synopsis or summary of what this novel is all about. The average reader will be able to do this without memorizing the tens of thousands of words but simply by applying a cultural schema like the one we are suggesting for the analysis of our interviews. Applying the cognitive schema of a story, the reader will be able to identify the main characters, their intentions, desires and the actions that flow from these intentions. S/he will also be able to take into account the contextual aspects of the story.

Another example can be taken from autobiographical accounts. Telling your life history you will do so by presenting your actions as motivated; things happen to you, you try to make sense of them (develop an internal response to the world), then you act upon the world (producing an external response), which in turn again changes the state of the world you act upon, and so on.
Taking these elements (episode, event, reaction, change of state, internal and external responses) allows for the construction of a kind of generative grammar to identify stories in interviews and to parse large chunks of text into meaningful typified units. As mentioned above, one of the main advantages of this approach is that we do not have to stick to the literal transcripts (or the linguistic surface structure), but can look for the elements of episodes in the interviews. These elements can be expressed in different languages. Nevertheless, the interviewers were instructed to mark and respectively transfer important specifics like irony and country-specific references whenever applicable.

Producing these kinds of stories also requires a specific elicitation strategy when conducting the interviews, motivating respondents to report what happened to them, and how they encountered real world situations. Even when respondents do not report about their own experiences of relevant situations but remain at the level of general statements about the state of the world, these statements can often be read as stories in the sense of the model.

Using this approach one can develop a ñpragmaticò (in the linguistic sense) understanding of interviews. The respondent always performs as a communicating agent, informing the interviewer and trying to make him- or her-self understood in the social situation of the interview, giving information about the world and linking this with personal motives, plans and attitudes. The key point here is that these attitudes are not stand-alone constructs but tied into the communicative pragmatic course of the interview unfolding in time.

The graphical representation below gives an idea how stories can be parsed into their constituent parts:

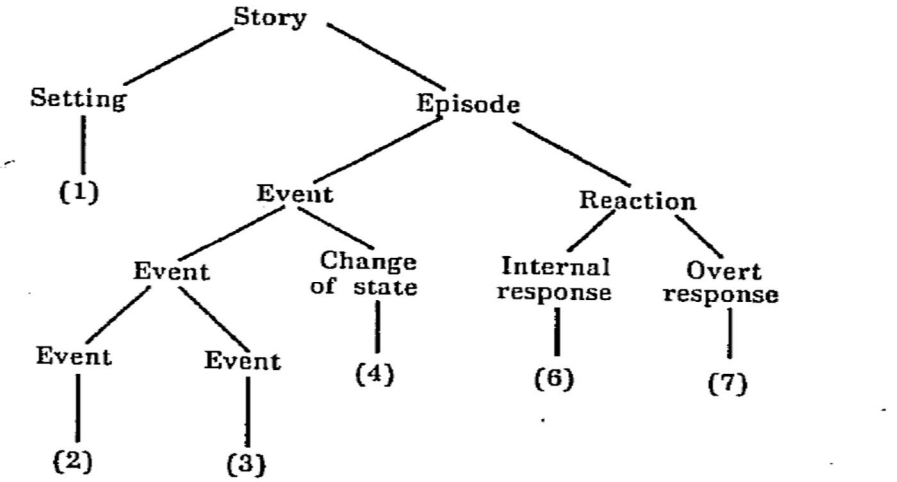


Fig. 1b. The syntactic structure of the story.

(From Rummelhart, 1975)[4]

Consider the following paraphrase of an interview:

(1) Sometimes I do shopping on the Internet (= setting)
(2) I buy a product using an online shop (= event)
(3) They ask for my data and I give them the information (= event)
(4) They send me a voucher for another Internet shop (= change of state)
(6) I have the opportunity to save money. I think this is a treat (= internal response)
(7) I order a product from the new shop using this voucher. (= overt response)

The story goes on and the respondent complains about all the advertisement mails being dumped into her mailbox from the new shop and from others offering similar goods (although no transaction took place with these other shops). This further course of events could also be parsed in a similar way.
Such individual stories can be made comparable, documenting different scenarios and the reactions of the respondents. In the brief example above, the story could be typified as a story of ñconsumer seductionò (lines 1-7), and then in the text below as a story about the nuisance, which is the price for using the ñspecial discount offerò (being dumped with spam offers). In the course of the interview the respondent answers that she does not know exactly whether these practices are legal, and she also does not know what she can do to stop it.
Parsing the interview in this way yields a sequence of nested stories, creating the image of an actor involved in different events, struggling with competing desires and needs, surrendering to the constraints and demands of the Internet (or developing strategies of resistance and resilience). *Attitudes* and *beliefs* do come into play here, but they are contextualized, embedded in practical everyday life actions

[4] Rummelhart, David, Notes on a schema for stories, In: Daniel Bobrow and Allan Collins, *Representation and Understanding, Studies in cognitive science,* Berkeley, University of California, 1975, p. 211-236.

1.2 THEORETICAL ASSUMPTIONS INFORMING THE WORK IN WP4

The sampling method

Interviews were conducted in five countries, using different entry points for the selection of interview partners. These different entry points were chosen to cover a number of social settings that seemed of specific relevance for our theoretical questions. In each of the five countries ï Austria, Germany, Italy, Slovakia and United Kingdom ï we attempted to recruit citizens specifically interested in one of the four areas that were chosen as entry points. These fields of recruitment were: crime prevention, e.g. individuals who were active in Neighbourhood Watch groups; consumer protection; workplace surveillance (e.g. active members of labour unions); and individuals from NGOs active in the field of data-protection. Furthermore in each country interviews with randomly selected citizens (control group) were conducted. This selection strategy was informed by the idea that citizens active in one of the above mentioned fields would have a specific understanding of different dimensions of surveillance. With around 45 contacts in each of the five countries we collected far more than 200 interviews. These interviews were parsed into 1000 stories addressing different topics. (A detailed description of the sample can be found below at the end of this introduction).

The conceptual framework

Surveillance and *resilience*, as the key concepts of our research, cannot be considered as household words for the average European citizen. Despite the recent public debate in the wake of the Snowden revelations we assume that only few people organize their daily lives on the basis of the fact they are (or could be) constantly surveilled. Although survey research suggests that many citizens do not approve of mass surveillance, one should not jump to conclusions about everyday behaviour on the basis of answers to explicit survey questions. Being tied into a dense net of data gathering in the most mundane of daily endeavours it would most probably foster a paranoid attitude to constantly consider the surveillance potential of every move one makes. Citizens use mobile phones, loyalty and credit cards; they register via e-government portals, make transactions through online shops and pass under CCTV cameras. It would be easy and inexpensive to monitor an individual in a society of electronic mass surveillance. As Bankston and Soltani have calculated, to monitor a person electronically costs 6.5 cents per hour, as compared to 275 $ when doing a covert operation with police officers.[5] What this demonstrates is not only the pervasiveness of surveillance but at the same time a quasi-ontological shift in human existence. Human beings, at least in Western societies, have become data subjects, continuously leaking information collected and stored by anonymous institutions or corporations.

Hence, from a theoretical perspective we suggest to give up the crisp distinction between the *social* and the *technical*. Whereas much of the surveillance studies literature operates with the (mostly implicit) categorical distinction between a social world and technical systems or assemblages operating on the social,[6] we suggest concepts like *techno-social hybrid* and

[5] Bankston, Kevin and Ashkan Soltani, Tiny constables and the cost of surveillance: Making cents out of United States vs. Jones, *The Yale Law Journal online*, 2014.
http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones
[6] Haggerty, Kevin D. and S. Ericson, ôThe surveillant assemblageô, *The British Journal of Sociology*, 51, No. 4 2000, pp. 701ï 717.

socially mediated technology.[7] Whereas it is common understanding among social scientists working in the field of surveillance studies that technologies incorporate a certain social/cultural concept of order (e.g. an algorithm for the detection of ñuncooperativeò individuals reflects and incorporates an idea of socially normal behaviour), the idea of a human as a composite techno-social hybrid unit is not as common in social theory and research. Gregory Bateson once used the nice example of a blind man and his stick, asking where the organism ends ï at the hand or at the end of the stick?[8] The same case could be made for glasses (even before the age of ñGoogle Glassesò), hip implants or cardiac pacemakers; but also for mobile phones or laptops.[9] The core point is to understand the ñmodern Humanò as a technologically mediated and supported form of existence.

This has consequences for the conceptualization of surveillance since it points to surveillance practices outside the narrow realm of law enforcement and crime fighting. Often surveillance is perceived primarily as a police practice, applied to prevent or apprehend suspected criminals. A central issue in the public debate about surveillance is the idea of a trade-off or balance between security and privacy. A standard argument in dominant discourse claims that an increase in security (through surveillance) can be achieved when giving up ñsomeò privacy rights. Citizens are asked to trade-in their privacy, provide personal data and accept highly intrusive surveillance measures to prevent criminal or terrorist attacks. While the evidence for this claim is shaky and the balancing metaphor is flawed[10] it nonetheless shapes and narrows the debate about surveillance to practices originating in the domain of public authorities (from secret services to the police). Although the public interest has shifted in the recent past the main focus of critical debates about surveillance is still on the citizen-state relationship. The loosening of legal constraints, the extension of state powers are objects of continuous critique.

Background information and theoretical remarks

At the same time processes of datafication in the realm of civil society, transforming citizens into leaking data containers and fostering the growth of hitherto unprecedented collections of person related data, go comparatively unnoticed in public debates. Considering these mundane processes of data-leaking and data collection, traditional surveillance measures in the context of state practices are dwarfed. Modern communication technologies integrated into everyday life in contemporary Western societies have seduced citizens into a kind of cyber-exhibitionism. Whereas requests from public authorities to provide person related information often encounter critical resistance, users willingly give away such information in other contexts. The most prominent examples are social media services like Facebook, providing a low threshold and free of charge platform for the presentation of self in cyber space. The often rehearsed critical phrase ñIf you donôt pay for a service you are the productò

[7] Comp. Brown, Sheila, Criminology of hybrids: Rethinking crime and law in technosocial networks, *Theoretical Criminology*, Vol. 10, 2, 2006, pp. 223 ï 244.
[8] Bateson, Gregory, *Mind and nature - a necessary unity*. Cresskill, N.J., Hampton Press, 1979.
[9] Comp.: United States: Supreme Court of the United States: Riley versus California, 2013. http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf
It states:ñ*A conclusion that inspecting the contents of an arresteeôs pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.ò p.15.*
[10] Comp. Berglez, Regina and Reinhard Kreissl, Report on security enhancing options that are not based on surveillance technologies, *SurPRISE Deliverable 3.3*, 2013. http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D-3.3-Report-on-security-enhancing-options-that-are-not-based-on-surveillance-technologies_v069.pdf

highlights the logic of the new data-economy underlying this development. Users pay for the services they use with personal information produced while using the service and harvested for further processing by the provider.

The ótraditionalô business model of commercial providers in the domain of social media is based on the idea of targeted marketing and advertisement. Selling third parties, i.e. other companies, the service to target potential customers and placing banners popping up on the screen of the target group creates the main revenue of Facebook, Google and the like. The service is ñfreeò for the users (who pay with their data) and the provider creates highly sophisticated profiles from individual usersô data, providing not only the basis for targeted marketing but also creating an ever-growing number of Big Data strategies, even including manipulative experiments.[11]

While the idea of selectively offering goods and services to individual users may look like a trivial extension of pre-digital customer relation management (CRM) practices, the sheer amount and diversity of data leaked by users opens up qualitatively new opportunities to create what could be termed ñconsumer intelligenceò at the individual and collective level. Based on the analysis of easily accessible information from individual users, (information that at face value appears to require no specific protection with regard to privacy), highly sensitive conclusions about private and personal traits of individual users can be produced. Recent research has demonstrated how sexual orientation, political preferences or personality traits can be derived with high reliability from an analysis of Likes and Dislikes posted on Facebook, or how individuals can be identified through an analysis of anonymised geo-location data from mobile phones. At the collective level a new kind of epidemiology is emerging based on the analysis of individual user information. Analysing traffic on Internet platforms or using linguistic analysis the spread of a flu epidemic can be followed in real time and early warning signs for changes of collective sentiments can be developed. Research conducted by Zittrain and others show, how Facebook is already considered capable of influencing elections.[12] In some cases intelligence services even try to counteract changes or manipulate public perception through targeted undercover attacks on e.g. online polls.[13]

These developments can affect citizens in many different ways without them being aware of the underlying processes of Big Data, data analysis, or even manipulation inhabiting the virtual world of cyber space. Cyber space itself constitutes a major source of information and orientation for an increasing part of the general population, where individuals move (act, live) in an environment shaped by interests and strategies not overtly identifiable or made public. In this virtual universe they are exposed selectively to information delivering the basis for their orientation, living in a world moulded by forces they do not understand and/or are not aware of. Moreover, it is highly likely that even allegedly objective information is individually filtered, based on former choices and preferences.[14] The situation resembles the plot of Hal Ashbyôs movie ó*Being there*ô, where Peter Sellers as the gardener in a wealthy manôs household exists in a secluded and virtual world with television as the only information

[11] Meyer, Robinson, http://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

[12] Zittrain, Jonathan, http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering

[13] Comp. Gleenwald, Glenn, https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/

[14] Pariser, Eli, *The filter bubble. What the internet is hiding from you,* Penguin, New York, 2012.

channel to the outside ñrealò world. After his employerôs death he has to leave the house and is exposed to the real ñrealò world where he attempts to handle emerging problems using the remote control panel of the TV set trying to switch between channels. A similar shift is taking place in the everyday lives of modern citizens. An increasing part of their mundane world knowledge is derived from Internet sources and the mingling of virtual and physical experience creates interesting new attitudes towards the world.

A second important assumption for the theoretical underpinning of our analysis is the starting point of *interaction* as a basic category, as opposed to the isolated individual or actor. Being ñhumanò is primarily a social form of existence, i.e. the central unit of analysis in social research should be the dyadic pair (or the group) and not the isolated individual as bearer of beliefs, attitudes, or habits. Combining these two aspects ï merging the social and the technical, and taking interaction instead of individual action as the starting point ï the problematic of surveillance and technology can be reconstructed in a comprehensive way. Starting from the dyadic constellation points to an important dimension for the analysis of surveillance: *the relations of communication*.
In a trivial sense communication has been one of the main targets of surveillance from the very beginning. The massive interception of Internet traffic, telephone conversations and other forms of communicative exchange between individuals and organisations has triggered heated debates about the right to privacy in personal communication. With the global spread of digital electronic communication media, organisations like NSA or GCHQ access communication deemed private to a hitherto unprecedented extent.
But at the level of everyday life the technologically mediated changes of the relations of communication can produce a number of effects not immediately linked to surveillance in the sense of eavesdropping. Being constantly online due to mobile phone and E-mail switched on 24/7, with a low threshold for accessibility for third parties, transforms patterns, routines and standards of communicative exchange.

From a theoretical perspective this can be analysed as a decoupling of proximity and intimacy. As authors like Alfred Schütz have demonstrated, the social world is comprised of what Schütz called different provinces of meaning.[15] Developing his analysis in pre-digital times, Schütz focuses on the immediate world ñwithin reachò as the prime source for an actorôs experience of the world. With growing (physical) distance objects and individuals become less tangible and remote. Such structures of the life world, extensively analysed by social phenomenologists, are changing with the advent of electronic communication media. New communities and new forms of intimacy can emerge uncoupled from the constraints of physical space. New forms of co-presence and exchange are made possible in the realm of the virtual. This affects also the notion of privacy. The private sphere no longer is co-extensive with a space of physical proximity but has to be reconceptualised on the basis of data protection in a much wider sense.

This may sound rather abstract (and it probably is). But in the overall context of IRISS we strive to go beyond simple ideas like privacy, defined as a category applicable to isolated individuals (or legal subjects, endowed with fundamental rights). Conceptually the analysis in

[15] Schütz, Alfred, *The Phenonemology of the Social World.* Northwestern University Press, Evanston IL,1967.

WP 4 will focus on interaction, exchange, embedded action or social action in context. Privacy then is rather to be applied to social constellations, which in a way may be a truism, but could help to clarify the theoretical status of the concept.
The basic intuition informing the analysis in WP 4 is that ñtechnologyò injects a new element into the social, transforming it in many (often unpredictable, unforeseen, under researched) ways. In social theory writers like Zygmunt Bauman elaborated extensively on the liquefaction of the social. Modern communication technologies (at the consumer/user end as well as at the level of infrastructures) do play an important role in that process of such liquefaction. Bauman is referring to the changes in the basic categories of time and space, which are used to provide structure to the social.[16] Nikolas Rose has suggested extending the (cultural, political) idea of citizenship towards what he terms ñbiological citizenshipò,[17] introducing notions like bio value or ñbiosocialityò borrowed from Waldby and Rabinow[18] respectively. In a similar way one could think about a kind of technological citizenship and introduce the concept of techno-sociality or information value and perceive of humans as machine-readable techno-social hybrids.[19]

What WP 4 investigates are the many mundane situations where citizens in their ñliquefiedò existence are governed by surveillance, i.e. how the social flows and individual access to goods and services are controlled by means of surveillance practices, directing movements, excluding and including individuals on the basis of their information value. We collected stories about how people relate to the fact of being techno-social hybrids. Of course a concept like techno-social hybrid is not used for self-description. It is a term for the interpretation, used to understand when and where humans are linked to technology and technologically mediated surveillance.

The focus of WP 4 is on the reconstruction of the multiple ways surveillance, mediated by new technology, is embedded into the fabric of society and shapes social relations. This can be achieved by looking at what at a first glance may look like idiosyncratic micro-events on social ground level.
With regard to the analytical perspective, what we are interested in is the citizensô point of view. There are the most incredible technological systems operating in the world, many of them hidden and unnoticeable, but nonetheless affecting the everyday lives of the general population.

Interdependencies within the IRISS project
In doing this we are connecting to the ideas about the social perspective on surveillance of our theoretical framework of IRISS, developed in WP 2:

> ***ñ****The essences of the social perspective are the social implications and consequences of surveillance technologies, including the way that human relations evolve with the diffusion of new technologically mediated surveillance systems and practices. At the*

[16] Bauman, Zygmunt, *Liquid Modernity*, Politiy Press, Blackwell, Cambridge, UK, 2000.
[17] Rose, Nicolas and C. Novas, *Biological citizenship*. Blackwell Publishing, 2004.
[18] Rabinow, P., Artificiality and enlightenment: from sociobiology to biosociality, *Essays on the anthropology of reason*, Princeton University Press, NJ, 1996. Waldby, C., *The visible Human Project: informatics bodies and posthuman medicine*, London; New York, Routledge, 2000.
[19] Brown, Sheila, The criminology of hybrids: Rethinking crime and law in technosocial networks, *Theoretical Criminology*, May 2006, 10: pp. 223-244.

heart of this perspective is a recognition that surveillance technologies interact with and shape (and are shaped by) societal structures, institutions and relationships. The focus of the social perspective is therefore «the social», how humans interact and relate to one another and with new technology. The underlying theme emerging from this perspective is that surveillance, mediated by new technology, is increasingly embedded in the fabric of society, and as such shapes and is shaped by social relations and structures.»[20]

The work in WP 4 provides the empirical underpinning for the theoretical propositions developed in the preceding Work Packages.

1.3 OPERATIONALIZING SURVEILLANCE EFFECTS

As mentioned above the approach chosen in WP 4 is to understand citizensô perspective on living in a surveillance society in their own words. We can and have identified in IRISS a number of technologies and practices affecting the lay citizensô life in many different ways. We then started to elicit stories from respondents about technology use and their personal views. These accounts and narratives then had to be analysed and interpreted against a theoretical background. We identified a number of problems, tasks, or dilemmas each individual living in a surveillance society is facing and tried to read the stories we received in our interviews as attempts to ñsolveò these problems, manage the tasks or come to grips with the dilemmas.

One of the basic problems citizens as techno-social hybrids face in surveillance societies is the task to actively provide for their privacy. We assume that privacy no longer can be assumed to be the default state in surveillance societies. We used the term *privacy labour* to account for this problem. We conceive of privacy as a cultural category informing social practices and defining behavioural obligations in daily life. Entering another personôs house without being invited to do so would have been considered a breach of privacy. Reading letters addressed to a third party, peering into oneôs neighbourôs window, intentionally listening to private conversations or making private information publicly available without consent ï all this would constitute a breach of privacy in the traditional sense. The crucial point though is that such breaches typically require an activity on the side of the ñbreachingò party. In the age of electronically mediated communication and new social media, this changes in several respects. Person related information is documented automatically in a myriad of databases (such as consumption and shopping habits, browsing histories, etc.). On social media platforms like Twitter or Facebook an individualôs data, communication and images are made available to a more or less unlimited number of viewers and readers. The image of a leaking data container, frequently used in surveillance studies nicely captures this situation: each technology-mediated individual action produces data leaking ñinto the openò. Many trivial daily actions are of this kind: using loyalty cards, mobile phones, social media platforms, electronic banking ï shopping, communicating, paying bills. All of these activities

[20] IRISS *Deliverable 2.4,* Comparative theoretical framework on surveillance and democracy, p. 12.

produce person related data leaking from the private sphere of the individual into virtual space.[21]

At the same time, injecting technologies into everyday life changes many routine activities, increasing convenience, lowering thresholds, providing a wide array of options at the tip of oneôs finger. All this entails data exchange, and affects a personôs privacy, but at the same time there is an increase of convenience. So from the perspective of our analysis in WP 4 we construe the dilemma of convenience vs. privacy. How do citizens handle this dilemma? Are they aware of it? Is it reflected in the narratives they produce? These are the kinds of questions addressed in the analysis.

While the trade-off between privacy and convenience may become obvious only upon reflection, the dominant discursive frame in public and policy debates about surveillance addressing the trade-off between *privacy and security* is a constant topic of political controversy[22]. The basic idea behind this trade-off or dilemma is rather simple: increasing surveillance in society by means of more technologies and control measures will help to identify potential perpetrators; identifying perpetrators before they can do any harm (plant a bomb, commit a crime) will increase the security of citizens. This simplistic reasoning is based on a number of problematic assumptions about surveillance, criminal actors and the inner workings of law enforcement agencies. Nonetheless it is widely accepted when it comes to the introduction of surveillance technologies, legislation or control procedures targeting the general public. In the interviews conducted in WP 4 we elicited stories from respondents about their experiences with different surveillance assemblages, trying to identify if and how they reacted to the fact of being surveilled. The majority of stories we identified were from the perspective of the watched, i.e. from individuals exposed to different surveillance technologies; but we also identified a number of stories narrated from the position of the watcher, i.e. from individuals practising surveillance while watching others in different institutional or organisational contexts. What we sought to identify in the analysis are different types or forms of reactions towards surveillance measures, designed to increase security (e.g. CCTV in different public spaces). With this analysis we could reconstruct a large variety of sometimes highly complex and contextual readings of individualsô awareness of living in surveillance societies. This also entails a number of resilient reactions ï from straightforward resistance to explicit avoidance of being exposed to surveillance. Looking at individual reactions to surveillance measures that are justified with the need to increase security, reveals a number of highly reflective interpretations of surveillance regimes among our respondents. Although we cannot generalize or draw any substantiated conclusions about large populations on the basis of our data, we are able to demonstrate that individuals develop highly sophisticated and unexpected forms of dealing with surveillance measures, based on sometimes highly elaborated interpretations of the technology and its uses for security purposes.

[21] see Carr John et al., Hitting the moving target: challenges if creating a dynamic curriculum addressing the ethical dimensions of geospatial data. *Journal of Geography in Higher Education, 2014,* publ. online.
[22] see e.g. Anderson, Malcom, Jean Carlo and Apap Joanna: *Striking a Balance between freedom, security and justice in an enlarged European Union.* Brussels, 2002; Heymann, Philip B. and Juliette N. Kayyem, *Protecting Liberty in an Age of Terror*. Cambridge, Mass.: MIT Press 2005.

As opposed to the constellation of being watched as an individual from an unknown third party, i.e. being under surveillance from outside, a different scenario emerges when looking at the changes in what we term the relations of communication. Here we can observe a trade-off or dilemma similar to the one mentioned above between privacy and convenience. Shifting the daily mundane communicative exchange from face-to-face encounters onto the platforms of social media can make trivial chats accessible to undisclosed audiences. While some basic privacy settings may be adjusted to create a kind of private zone the new cultural practice of ñpostingò information on the Internet produces new communicative formats and changes the relations of communication. A person might want to share a piece of information (a string of text, an image) with others in a non-directed way, i.e. it is not Ego addressing Alter in a one-to-one interpersonal relation, but Ego posting-addressing a broader audience the limits of which are unknown. Since this audience is not physically present, its size may be irrelevant for the individual. New formats like Twitter, operating with the model of ñfollowersò are specifically designed to communicate with a larger public: the higher the number of followers, the higher the prestige of a person. Barack Obama, President of the United States has around 45 million followers for his Twitter account.
While the mundane notion of person-to-person communication may be based on the idea of physical co-presence and a shared, more or less intimate space, the electronic infrastructure of ICT-enabled communicative exchanges creates completely new boundaries, formats and forums.
We tried to capture these changes as a dilemma of *privacy and sociality*, investigating citizensô reactions and responses to the very fundamental changes in the relations of communication brought about through ICT and the surveillance potential these new technologies entail.

Asking respondents about their everyday use of modern technologies, one area that we frequently touched upon in our interviews was the use of these technologies at the individualsôworkplace. Controlling the workforce by means of more or less sophisticated and rigid surveillance regimes is a practice emerging with the modern form of production in the factory. Technology changes the work processes and at the same time creates new opportunities for management to monitor and control performance and behaviour of employees. Some of these monitoring practices may be justified with the need of improving workflows and optimizing processes and use of resources. But surveillance can reach far beyond what could be termed functional needs of optimization and intrudes into the privacy of employees in a hitherto unprecedented manner. The ensuing surveillance practices sometimes resemble the highly problematic practices of law enforcement agencies ï like monitoring electronic mails of employees ï and in our interviews, respondents were highly concerned about these practices. On the other hand being employed involves an asymmetrical power relation, i.e. while our respondents were aware of the probably illegal nature of privacy intrusions going along with surveillance at their work place, they at the same often surrendered to these practices since the only viable alternative would have been to quit the job. The use of surveillance technologies at the workplace displays the general problematic of the surveillance society in a nutshell: traditional relations of trust between the involved parties are replaced and eroded by surveillance, the implementation of new ICT paves the way for multiple forms of function creep and the existing power relations between employer and employee are changing in many different ways. From the perspective of the respondents in

the interviews we conducted one of the main dilemmas was the *relation between privacy, trust and fairness*. Surveillance practices at the workplace replace traditional relations of trust and the amount and intensity of surveillance raises concerns with regard to fairness: the stories we received in our interviews are often moral stories addressing the legitimacy and adequacy of surveillance practices, shaping the work environment and restraining what is perceived as legitimate areas of freedom and privacy.

The final constellation we addressed in our analysis involves citizens as active agents in a surveillance relation. Prototypical cases for such relations are provided by neighbourhood watch schemes or any attempts of citizens to increase what could be called local security by active engagement in surveillance practices. Grass root activities like Neighbourhood Watch can also be interpreted as a form of bottom-up resilience, i.e. a joint effort by citizens to increase the (perceived) security in their neighbourhood. Surveillance in different forms is a key element here, from video cameras installed on private premises to volunteer citizen patrols searching for suspicious individuals in the streets. Stories about Neighbourhood Watch are different in different countries. This is due to different cultural traditions of policing and law enforcement. Whereas in the Anglo-Saxon context citizen involvement has a long tradition, continental societies like Germany, Austria or Italy did never develop this kind of active vigilantism. In post-authoritarian societies like Slovakia the recent political transformations create a very specific situation, where ideas like Neighbourhood Watch do not resonate well with public understanding of crime fight and security. With regard to privacy and security a core dilemma emerging here is the trade-off between individual freedom and communal supervision (or surveillance for that matter). Neighbourhood Watch schemes often emulate a rural village-type social climate, where everybody should know everybody else in the neighbourhood and also watch over his or her neighbour. The downside of this sometimes over-romanticized image is very dense and rigid control among local residents ï social theorists like Walter Benjamin and Georg Simmel praised the anomie of city life and the individual freedom it entails.

1.4 METHODOLOGY: THE INTERVIEWING PROCESS AND THE DATABASE

Regina Berglez

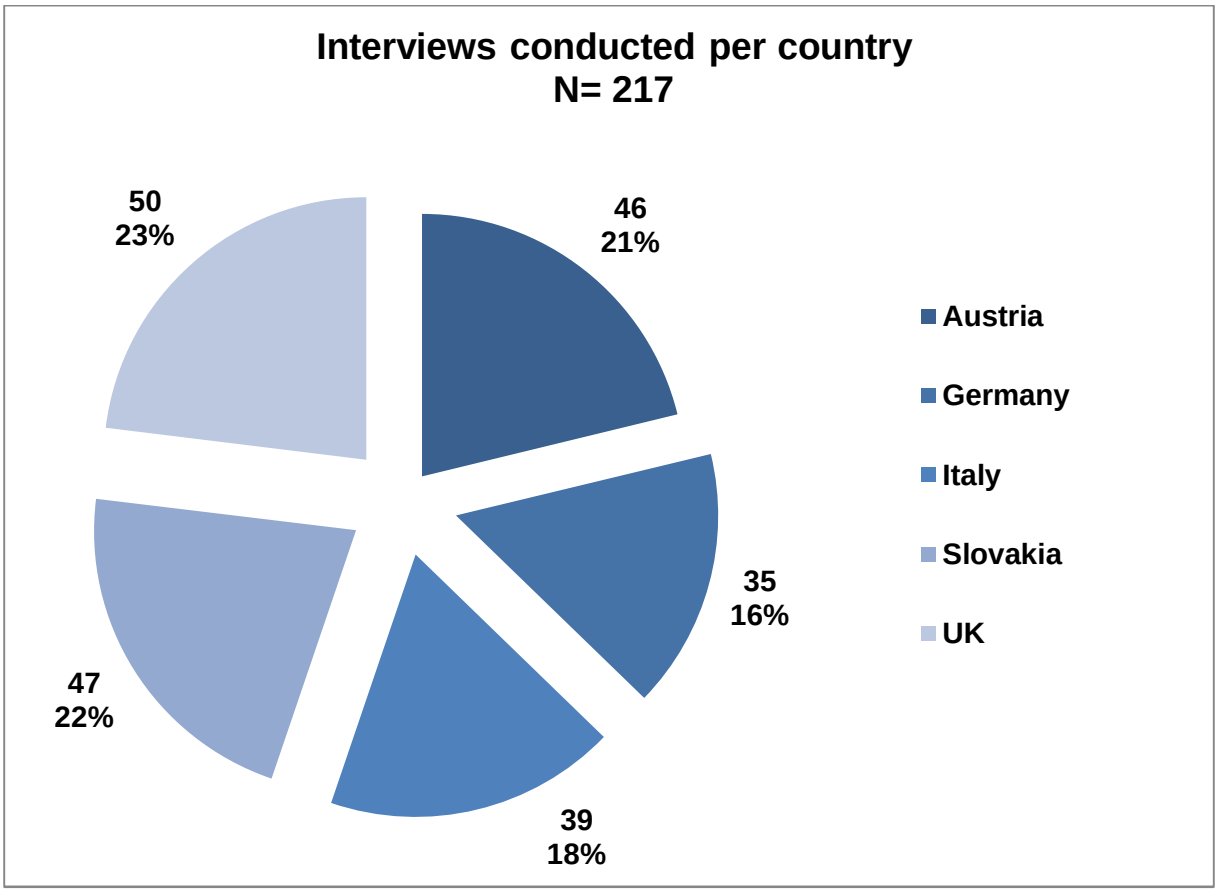
In the course of the WP4-fieldwork until December 2013, a total number of 217 open and elaborate personal interviews were conducted. The five involved countries are: Austria, Germany, Italy, United Kingdom and Slovakia.[23]

The interviews

Citizens were partly recruited on the basis of their particular interest in or their special experiences with a number of topics listed below. In order to compare this deliberately biased sample with unbiased respondents, however, the largest group in the sample was the random control group that was not recruited on the basis of any particular experience or engagement.

[23] For further details on recruiting and the interviewing process see: ñGuidelines for the participant observation and interviewsò, IRISS Deliverable 4.1.

The distribution of interviews across the involved countries is as follows:



The recruiting topics were:

- Surveillance as a side effect of consumer culture
- Privacy and data protection
- Control at the workplace
- Neigbourhood Watch and the like

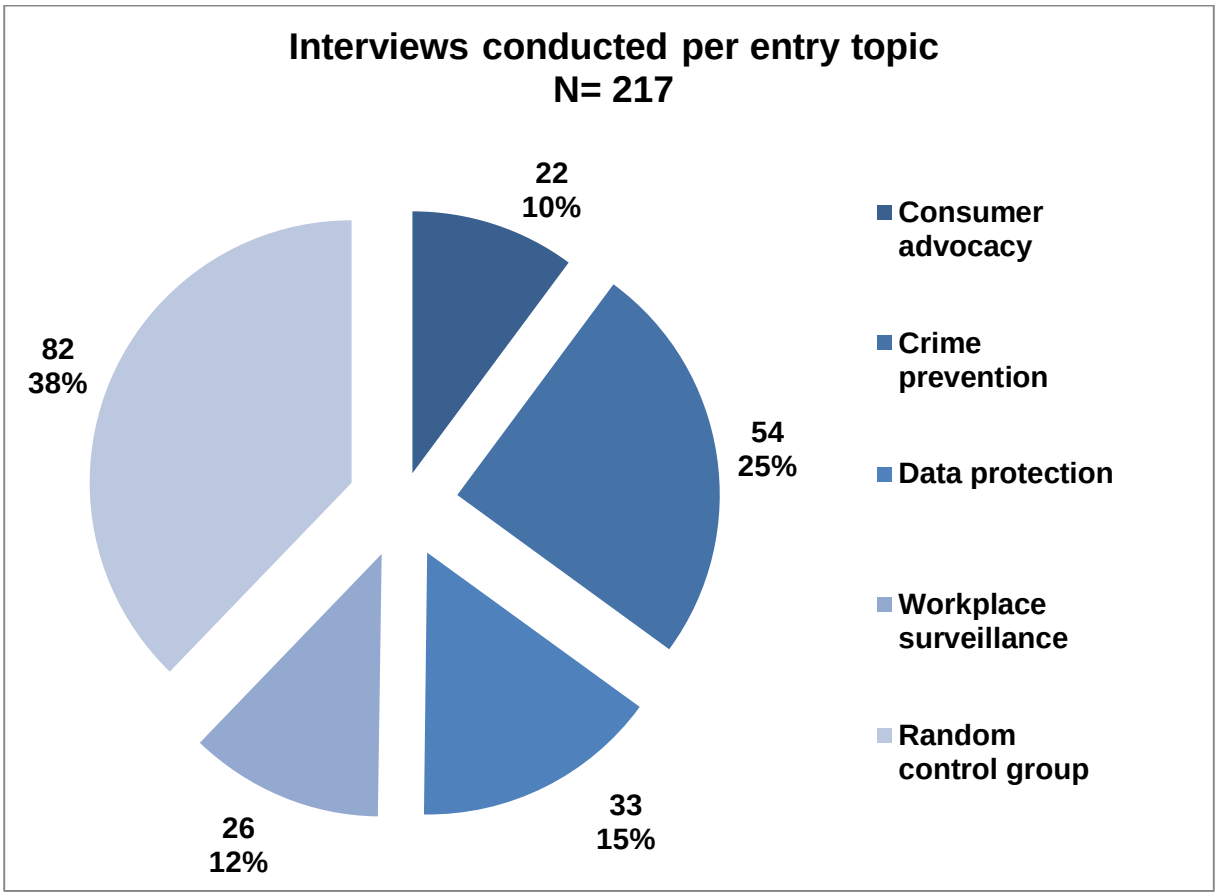
Nevertheless and of uttermost importance is, that in all of the 217 interviews a standardised interview guideline was used consistently.[24] Although the emphasis of a particular interview varied according to the interests and experiences of the respective participant (as above), the five main overall topics were, however, in every interview circumstancially addressed.

These five overall themes (ćtopics in IRISSô) within the course of the interviews were:

- Crime prevention
- Workplace surveillance
- Consumer advocacy
- Data protection
- (General) questions on surveillance, privacy and control

[24] See Annex II

The distribution of interviews conducted per entry topic is as follows:



Also, so as not to trigger an immediate association with surveillance, initial warm-up questions used in the interviews were expressed along the lines of ñ*What comes to your mind first when we speak of modern technolgy***ò**.

The timeframe of the individual interviews varied from around 40 minutes (as the minimum) up to a maximum of 90 minutes. The timeframe estimated for an interview at the outset was one hour, to which the majority of the interviews conformed and which has also been the average interview length.

All interviews were

- ŏ electronically documented
- ŏ synapsed
- ŏ and summarised along the core questions
- ŏ produced in English,
- ŏ entered into an online-database (accessible to all partners involved),
- ŏ transferred into a master database,
- ŏ and recoded and structured (bottom-up approach)
- ŏ in accordance with our theoretical framework.

The database

The finalised master-database contains a total number of 1000 quotes that were extracted as narrative stories from the 217 interviews conducted.

As already stated in the previous chapters, we have identified a number of areas (or domains) with regard to the dominant dilemmas. These dominant dilemmas serve as the overall framework for the structure of our extensive final database and are as follows:

Privacy ï convenience	This dilemma is regarding the ótrade-offô in the domain of electronic commerce, that is the citizensô desire for convenience and the possible consequences of óBig Dataô that come along with electronic consumerism.
Privacy ï security	This can be seen as the political ómaster dilemmaô, as the basis of the óbetter safe than sorryô rhetoric, and is relevant in daily life in a great variety of different contexts.
Privacy ï sociality	Addressing the need to use social media in order to stay in contact with friends and colleagues while at the same time making personal information available for the service providers or a wider public is the core dilemma in this category.
Privacy ï trust/fairness	Stories about work-place surveillance, as well as stories regarding the general relationship between citizens and the state are subsumed under this heading.
Engagement ï security	This is a specific category for stories from and about activities in the field of Neighbourhood Watch and consists mainly of stories about the aim of citizensô to óincreaseô security.

The unit of analysis is always the quote ï also referred to as a story. A quote consists of a self-containing story from an interview and is therefore independent from the course of an/the entire interview. On average, one interview resulted four to five stories, although this varied, as can be the case with such qualitative approach.

Each of our 1000 stories is linked to at least one of these thematic categories (=main dilemmas), constituting the heuristic grid to structure the narrative data. In some cases it made sense from an analytical point of view to assign a quote to more than one category (e.g. if an interviewee telling a story about CCTV in the public sphere was at the same time problematizing the role of the state with regard to the cameras). This means, that there is either a one.-to-one or a one-to-many relation between categories and stories.

To clarify this point, a visual exemplification of the database (screenshot) of an extract regarding the coding structure for the various dilemmas is provided as follows.

Topic in IRISS:	e: Initials of perso	4. Convenie	4.x Sublevel (	5. Security (D	5.x Sublevel Se	6. Sociality (D	6.x Sublevel	7. Trust - F	7.x Sublevel Trus	8. Engage	8.x Sub	9. NSA Snc
Crime prevention				security						neighbourhood watch		
Crime prevention				security	crime prevention without NW							
General questions	RB							trust - fairness	relationship citizen-state			
Data protection						sociality	data protection					
General questions				security	CCTV							
Consumer advocacy		convenience	loyalty cards									
General questions								trust - fairness	relationship citizen-state			
Data protection						sociality	social media					
Crime prevention				security	victim experience							
General questions				security	CCTV			trust - fairness	relationship citizen-state			
Crime prevention										neighbourhood watch		
Workplace surveillance								trust - fairness	workplace surveillance			
Crime prevention				security	crime prevention without NW							
General questions						sociality	social media					
Crime prevention										neighbourhood watch		

Screenshot: section of the WP4 database

As can be seen, the main dilemmas were also categorized into sublevels. To some extent these sublevels also go along with the subchapters of this report (e.g. in a story belonging to the main dilemma ñtrust ï fairnessò the topic could regard the relationship between citizen and the state, or the topic might fall into the realm of surveillance in a work environment). Some of these ï obviously still rather generic ï sub-categories were then much structured further and deeper, i.e. they contain more than only the one sublevel per dilemma as is shown above, which was necessary in order to handle the database accordingly. The details of this complex coding process, however, do not need to be elaborated at this stage.

The classification (final coding) of the 1000 quotes into the five dominant dilemmas is as follows, adding up to a total number of 1048, since in 48 cases the quote was double-coded (as explained above).

- **Convenience**
  - 185 quotes
- **Security**
  - 299 quotes
- **Sociality**
  - 243 quotes
- **Trust - Fairness**
  - 273 quotes
- **Engagement**
  - 48 quotes

For clarification: the structuring into these five dilemmas should not be confused with the recruiting entry point of the interviewees, or with the variable ótopic in IRISSô. These three points/variables (recruiting topic; topic in IRISS; and the dominant dilemma) mark different information i.e. different stages in the course of the work process: entry points (recruiting), data collection (interviewing) and data structuring (coding).

Further information on the process of data entry and coding can be found in the condensed guideline in Annex II.

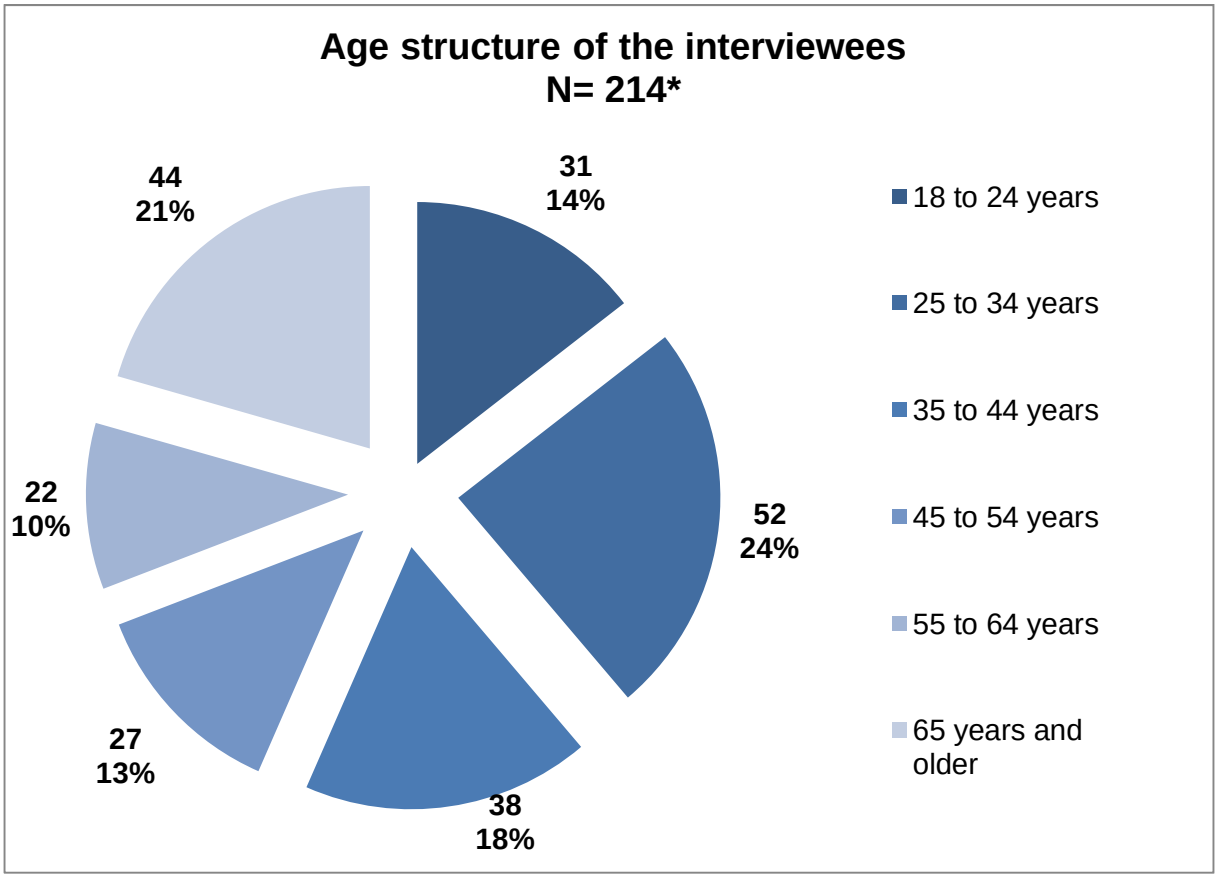
The participants

Gender:

The gender balance was almost perfectly representative: 51% of respondents were female, 49% were male. The gender distribution within the various age groups was also satisfactory.

Age:

The general age categories of the respondents are as followes:

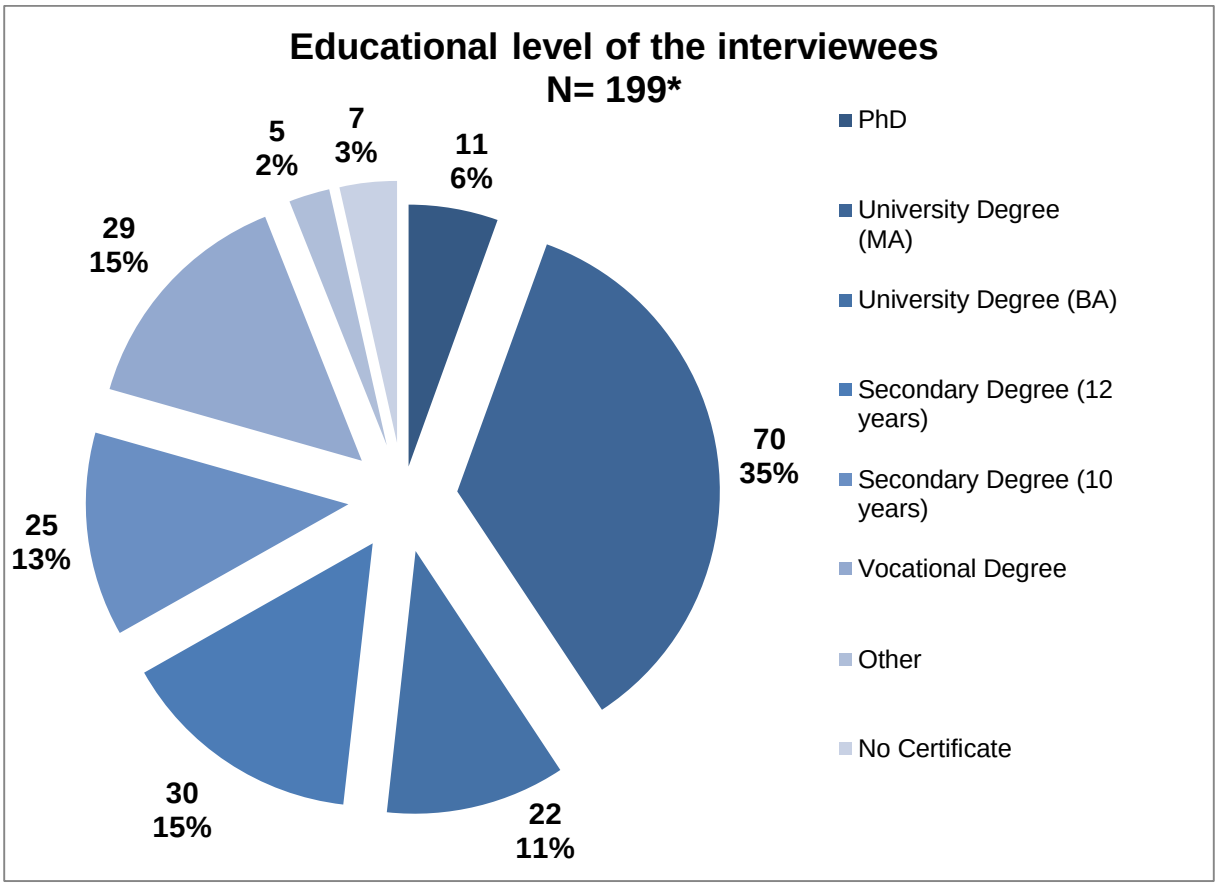


*3 missing

The distribution of the age categories can in generall be seen as satisfactory.

Education:

The educational level of the respondents is as followes:



*18 missing

The distribution of the educational level shows a slight bias toward higher academic degrees. This distortion is due to the sampling strategies applied to this research. Reseacher were snowballing respondents from their immediate social environment. Although we tried to cover a wide array of social demographic groups this copuld not always be fully achieved.

For a more detailed overview of the demographics of the interviewees see Annex II.

Overview on the fieldwork in a nutshell

- A total number of 217 interviews was conducted
- in five countries: Austria, Germany, Italy, UK, Slovakia.
- These 217 interviews resulted in a total number of 1000 different stories.
- The stories are the main unit of analysis in WP4,
- and were classified into five overall dilemmas and diverse subcategories
- that constitute the overall framework of this report.

1.5 CONSIDERING NATIONAL AND CULTURAL DIFFERENCES: THE CASE OF GOOGLEôS STREET VIEW

Alexander Neumann; Chiara Fonio and Alessia Ceresa, Martin Kovaniļ, Keith Spiller and Charles Leleux , Daniel Fischer

The research in IRISS WP4 was conducted in five different European countries: Slovakia, Italy, Austria, Germany and in the UK. Although the sampling strategy applied to recruit citizens in these five countries was the same (e.g. using the same field entry points) it can be assumed, that the perception of surveillance differs in different everyday contexts. To reflect on these assumed differences in the public perception of surveillance and to consider the different relevance that organisations involved in surveillance have, IRISS drafted reports on the involved countries. The country reports worked along research questions dealing with data protection and privacy sensitive issues such as the national implementation of the EU data retention directive (2006/24 EC) for example, which was in place while conducting the empirical field work in IRISS. The full length reports can be found in ANNEX I, this subchapter will highlight the case of Googleôs Street View for two reasons. In the narratives of individual experiences with different kind of technologies the respondents often referred to ñ*the Internet*ò as one of the most powerful sources of information and control. Control in the sense that through the various social media sites, citizens can watch other users but also be watch by other users and the services providers on the same page. As one the most prominent search engines, Google has a special role here.

The country reports[25] compared the national responses to the question of how Googleôs Street View (GSV) project was received in the respective national contexts? The research assessed public awareness and documented critical reactions. The results of the analysis on GSV implementation in the national context is summarised in the following table:

	Is Googleô GSV available in your country?	**Influence on the public awareness?**	**Which national association raised their concerns?**
Austria	No ï the national DPA stopped the GSV project	None ï There was a little interest in 2010, since then almost no coverage	ñARGE Datenò (a data protection organisation) and the Green Party
Germany	Yes	250,000 Objections against being mapped recorded by German DPA	Local government institutions (small towns), Politicians from all parties
UK	Yes	In 2009 almost no interest ï in 2013: considered as beneficial tool	ICO, Citizens stopping google cars, Privacy International
Italy	Yes	None - Limited	One consumer association
Slovakia	Yes	In general positive reactions by the general public, the media, the government and the DPA	None

[25] See Annex I

Google's Street View in Austria

Alexander Neumann

The Google Street View car was first sighted in Vienna in April 2009, recording data for their service.[26] However, 2 months earlier a similar service had already gone online, showing pictures from Vienna and, in further succession, other Austrian cities. This service is provided by a Romanian company – the eXtreme Soft Group S.R.L. – "the first "street-level imaging" service for Eastern and Central Europe."[27] Another similar service for Austria was provided by herold.at – the Austrian yellow pages – called "Herold Straßen-Touren" showing a GSV of the shopping areas in the federal state capitals of Austria and went online in July 2009[28] but doesn't seem to be available anymore.

Google registered the GSV application at the DPA in January 2010 with the plan, to go online sometime in 2010.[29] In spring 2010, information emerged that Google not only collected pictures but also non-encrypted data from wireless networks via their GSV cars throughout Europe. As a response to this, the Austrian DPA launched an investigation against Google resulting in a provisional ruling – issued end of May 2010 – that forbade Google to use any of the GSV data, including data collection.[30] Google appealed against the provisional ruling, declaring that no more WLAN data was beingcollected in connection with the GSV application.

The investigation led by the DPA revealed *"that the WLAN data had been collected for a different purpose than the one stated in the notification for "Google Street View" and should therefore not be regarded as a part of the "Google Street View" data application"*.[31] The ban was lifted on the 30th November 2010, although the examination regarding the use of WLAN data by Google is still running to date. This led to a new registration of the GSV application on the 21st April 2011 with three recommendations provided by the DPA to Google. Those recommendations state that: (1) Google must blur the entire image of a person in the entrance area of sensitive places (churches, prisons, etc.); (2) as well as images of private (fenced) properties, not visible to pedestrians; (3) and a suitable tool has to be provided, so a subject can object in a simple way to the data published by Google.[32]

Google stated that they were happy that their application had been registered, but that the GSV project has no priority in Austria and has been postponed indefinitely. To date. this status remains in place, as Google shows no intention whatsoever of resuming the collection of images and launching GSV in Austria, and the data previously collected remains in their

[26] Der Standard 9th April 2009 Google macht Österreichs Straßen unsicher http://derstandard.at/1237229445223/street-view-Google-macht-Oesterreichs-Strassen-unsicher 08.04.2013

[27] Der Standard 9th Februar 2009 Mit GSV-Klon Wiens Straßen erkunden http://derstandard.at/1233587023245/Ansichtssache-Mit-Street-View-Klon-Wiens-Strassen-erkunden?_slideNumber=1&_seite= 08.04.2013; http://www.norc.at/about-norc-help.html 08.04.2013

[28] Krone Zeitung 1st July 2009 Herold.at bietet virtuelle Straßen-Touren http://www.krone.at/Digital/Herold.at_bietet_virtuelle_Strassen-Touren-Shops_schauen-Story-151188 08.04.2013

[29] Krone Zeitung 13th December 2009 "GSV" soll 2010 in Österreich an den Start gehen http://www.krone.at/Digital/Street_View_soll_2010_in_Oesterreich_an_den_Start_gehen-Heimische_Strassen-Story-175686 08.04.2013

[30] Kleine Zeitung 27th May 2010 Österreich stoppt GSV http://www.kleinezeitung.at/allgemein/multimedia/2362022/boxenstopp-fuer-google-street-view-fahrzeuge-oesterreich.story 09.04.2013

[31] Case history "Google Street View" http://www.dsk.gv.at/site/6733/default.aspx 09.04.2013

[32] Conclusion of the proceedings regarding "Google Street View" in Austria http://www.dsk.gv.at/site/6733/default.aspx 09.04.2013

archives.[33] Recently, a few GSV pictures have been launched in Austria: Since April 2012 the Kunsthistorisches Museum (museum of Art History), the Leopold museum and the Albertina museum have included images from the ñGoogle Art Projectò in their collections and in November 2012 Google expanded GSV, showing pictures from ski resorts in Europe, Canada and the US, including Ischgl and Sölden in Austria.[34]
The main opposition against the GSV project was led by the Austrian working group specialized on data protection and privacy, the óARGE Datenô. Among others, they provide a long explanation on how to prevent a breach of privacy concerning GSV including a template cease-and-desist letter.[35] On a public level, there were no noticeable protests or actions against GSV. The only ï quirky ï case in Austria was the attack of a 70-year-old resident in Steyregg, a small town in Upper-Austria. At the sight of the GSV car, the resident wanted them to leave. As they didnôt react, he started to chase the GSV car with his pickaxe until neighbours overpowered him.[36] This happened in April 2010, around the time the GSV application was covered a lot in the media.

Googleôs Street View in Germany
Daniel Fischer

At the beginning of the project (in 2008 first pictures were taken by the GSV cars), there was protest especially in smaller town or villages all around Germany who tried to ban GSV cars from their streets. Even as the project became increasingly prominent, there were no institutional protests reported coming from bigger cities, but from many suburban communities with huge living areas consisting mainly of terraced or detached family houses. The only action taken by politicians at the federal level was the initiation of judicial examinations of the GSV case, which did not produce unanimous results: An expert opinion by the ñInstitut für Rechtsinformatikò states that GSV does not infringe privacy rights (23.2.2010), whereas other expertise obtained by the Ministry of Justice of Rheinland Pfalz considers the project partly illegal, e.g. because GSV-Pictures are taken above eye level and because ñraw data are exported to the US and further processing canôt be controlledò.37 In addition to this lack of clarity within data protection and privacy laws it also became evident that institutional responsibilities were not clear enough to deal with the issues brought up by GSV: German GSV-Project Manager Keuchel said that as of April 2009 there was one single office/person who was authorized to lead the discussions and bargaining with Google

[33] Futurezone 21st April 2011 Grünes Licht für Google Street View in Österreich http://futurezone.at/netzpolitik/2815-gruenes-licht-fuer-google-street-view-in-oesterreich.php 09.04.2013, die Presse 30th August 2011 Google: Google Street View noch länger nicht in Österreich http://diepresse.com/home/techscience/internet/google/689380/Google_Street-View-noch-laenger-nicht-in-Oesterreich 09.04.2013, der Standard 8th March 2012 Google: Vorerst kein Start von GSV in Österreich http://derstandard.at/1330390635488/Kartendienst-Google-Vorerst-kein-Start-von-Street-View-in-Oesterreich 09.04.2013.
[34] Der Standard 4th April 2012 GSV für Wiener Museen http://derstandard.at/1333185134991/Google-Plattform-Street-View-fuer-Wiener-Museen 09.04.2013, Google Europe Blog 28th November 2012 The real Mountain View: on the piste with GSV http://googlepolicyeurope.blogspot.be/2012/11/the-real-mountain-view-on-piste-with.html 09.04.2013.
[35] Google GSV ï Wie verhindere ich eine Verletzung der Privatsphäre http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=65120uap 09.04.2013
[36] Austrian Times 8th April 2010 'Google GSV' driver escapes axe attack http://austriantimes.at/news/Panorama/2010-04-08/22317/%27Google_Street_View%27_driver_escapes_axe_attack 09.04.2013
[37] http://www.spiegel.de/netzwelt/netzpolitik/googles-strassenfotos-gutachten-erklaert-street-view-fuer-teilweise-rechtswidrig-a-681084.html, http://www.merkur-online.de/aktuelles/politik/gutachten-google-street-view-illegal-652444.html

(Johannes Caspar).[38] Until that point, it had been an ñIrish stewò of European, national and federal law that could not provide a secure legal basis for claims of any party, and all political reactions where based on ñvague fears and lack of understandingò.[39]
The role of privacy or rather the scepticism against any form of data collection in Germany has been discussed in the preface. Some politicians (across all different parties) tried to profit from this historical and cultural fact and drew very fatalistic pictures to provoke even bigger resistance against GSV, after the start of the service was announced: ñNo Secret Service in the world would go for pictures like these as unabashed as Google. [They] already have personal profiles that are more precise than any government in the world can produce.ò[40] This was criticized by Data Protection Agencies, who called for a more pragmatic way of dealing with modern technologies and services like GSV. After long discussions a 13-Point Catalogue of requirements was presented to Google that had to be fulfilled before the service could go online. The main point was the right of every citizen to have pictures of his housing pixeled. In the case of apartment buildings, a request from one citizen suffices to have the house pixeled. Finally 250.000 houses were pixeled, far less than estimated by politicians, such as those cited by Aigner, above. Debates around GSV continued after the release of the service but the tables have turned: Pixeled houses are perceived as annoying and shameful by leading internet activists[41] and journalists.
The last episode of the GSV-case in Germany deals with the trouble caused by the fact that Google had collected personal data by coincidence, when using WLAN Networks to get more precise geographic data. As a consequence Google was fined 145,000 Euro in 2013.[42]

Googleôs Street View in the UK

Keith Spiller and Charles Leleux

Googleôs Street View was introduced in the UK in 2009 and it is reported that 96% of the UK is now covered by the mapping system.[43] One incidence in particular has raised more media attention around GSV than any other and this related to data collection. When recording GSV images Googleôs cars also recorded information from unencrypted domestic Wi-Fi traffic. The recording of this information only came to light when the Germany Data Protection Authority conducted an audit in 2010.[44] Google have stated that the capture of this information was óunintentionalô ï an engineer was blamed for installing this capability without the consent or knowledge of the organisation. The Wi-Fi information, it appears, was collected in every country that has received GSV mapping. In the UK, the Information Commissionerôs Office deemed the collection illegal and Google were instructed, by the ICO and a number of National Data Protection Authorities (including US, Ireland, France and

[38] SZ, 18.3.2010, page 2.
[39] http://www.spiegel.de/international/germany/steamrolled-by-google-street-view-internet-challenges-overwhelm-german-government-a-712106.html
[40] http://www.spiegel.de/netzwelt/netzpolitik/street-view-debatte-bruellen-gegen-google-a-676609.html
[41] http://www.zeit.de/digital/internet/2010-11/street-view-jeff-jarvis-verpixelung
[42] http://www.handelsblatt.com/unternehmen/it-medien/wlan-mitschnitte-datenschuetzer-verdonnert-google-zu-bussgeld/8103482.html
[43] See, http://crave.cnet.co.uk/software/google-street-view-to-cover-96-per-cent-of-uk-roads-from-tomorrow-49305236/

[44] Guardian 15 May 2010. ó*Google admits collecting Wi-Fi data through GSV cars*, http://www.guardian.co.uk/technology/2010/may/15/google-admits-storing-private-data, accessed 28 Feb 2013

Germany), to delete this information.[45] In November 2010 Google agreed to delete all Wi-Fi information collected, however by July 2012 Google had not deleted the information,[46] causing further concern to data protection authorities.

Indifferent attitudes to breeches of privacy are all too familiar in the UK, in this instance, while widely published the harvesting of data has not, as yet, lead to any convictions or even public debate on the illegally captured online private data. Moreover, non-sensitive personal data is often considered to hold little importance or relevance for most online users (Green and Smith, 2002, New Scientist, 2009); however, if GSV captured, for example, bank details or personal and intimate pictures or even information of national interest, what then?

On an associated issue, the introduction of StreetView has raised some moral, ethical and discerning issues, for example, highlighting the location of refuge centres or images of people exposing their buttocks ï these images were removed due to national media attention.[47] In the UK, the privacy of individuals photographed leaving less salubrious establishments has been questioned (the examples include people recorded leaving a sex shop and urinating in public),[48] but as yet no major objections have been raised as to the impact of StreetView; especially from those photographed or who have had their data recorded.

Googleôs Street View in Italy

Chiara Fonio and Alessia Ceresa

Googleôs Street View was introduced in Italy in 2008, along with implementation of the service in France, the first country with GSV outside the United States[49]. Critical reactions soon emerged from Adoc (*Associazione Difesa Orientamento Consumatori*), a consumer association, which has been involved in many campaigns (from transparency in banking to consumersô privacy) from the early 90s until the present. Adoc drew attention to the fact that the automatic face blurring technology employed by Google did not always function properly, as pointed out by consumers who claimed that their faces could be identified, and also to potential infringements of the Italian Data Protection Code[50]. The consumer association asked the Italian DPA to check which data were collected by Google cars.

---

[45] Daily Mail 27 July 2012, *Sinister truth about Google spies: GSV cars stole information from British households but executives 'covered it up' for year*, http://www.dailymail.co.uk/news/article-2150606/Google-deliberately-stole-information-executives-covered-years.html. New York Times 30 April 2012, *Data Engineer in Google Case Is Identified*, http://www.nytimes.com/2012/05/01/technology/engineer-in-googles-street-view-is-identified.html?pagewanted=all&_r=0. New York Times 1 Aug 2012, *Google Failed to Delete GSV Data in France*, http://www.nytimes.com/2012/08/01/technology/01iht-google01.htmlNewYork Times 22 May 2012, 22 May). *Google Privacy Inquiries Get Little Cooperation*. http://www.nytimes.com/2012/05/23/technology/google-privacy-inquiries-get-little-cooperation.html?pagewanted=all. All accessed Feb 2013

[46] Guardian 27 July 2012, *Google faces new GSV data controversy.* http://www.guardian.co.uk/technology/2012/jul/27/google-street-view-controversy Daily Telegraph 27 July 2012, *Google: we failed to delete all Streetview data. http://www.telegraph.co.uk/technology/google/9432518/Google-we-failed-to-delete-all-Streetview-data.html*

[47] Irish Times 10 Oct 2010, 10 Oct). Barefaced Cheek on Google Street View, *http://www.irishtimes.com/newspaper/...reaking42.html* USA Today 6 April 2007, Google's street-level maps raising privacy concerns. *http://usatoday30.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy_N.htm*

[48] See http://www.telegraph.co.uk/technology/google/5022390/Google-pulls-embarrassing-Street-View-images.html and http://www.express.co.uk/pictures/galleries/1469/Google-street-view-s-most-embarrassing-pictures

[49] http://en.wikipedia.org/wiki/Google_Street_View.

[50] http://www.adoc.org/notizie/4130/privacy-ecco-le-prime-vittime-di-google-street-view-per-adoc-a-rischio-la-privacy-dei-cittadini (Retrieved on March 14th 2013).

Besides Adoc, the TagMeNot[51] project raised privacy concerns from a different perspective, trying to enhance citizensô online privacy through a pre-emptive approach and a ñfree opt-out technology for pictures taken in publicò. In particular, TagMeNot is a QR-Code that can be worn or displayed outside a house in order that pictures are not ñput on the webò. The displaying of the TagMeNot QR-Code means that ñyou are asking to remove personal details and blur facesò[52]

However, the abovementioned critical reactions did not help to raise public awareness, as media coverage was both limited and fragmented. Despite the fact that the Italian DPA did launch an investigation of Google Street View and reacted promptly to complaints made by citizens and consumers associations, neither relevant public debates nor citizensô protests occurred within the national context. The level of awareness for privacy was so low that an Italian start-up even opened a website called Trail me up[53] in order to offer views of places all over the world out of GSVôs ñgazeò, places accessible only on foot, like national parks.

As mentioned, the Italian DPA launched an investigation requesting Google Inc. to provide information on its data gathering and data processing. In April and May 2010, Google Italy s.r.l. informed the authority that while collecting images through Google cars, both data on Wi-Fi networks and ñpayload dataò that were not protected were collected[54] from 2008. The letter by Google Italy s.r.l was sent a few months after the Italian DPA notified Google of the start of an administrative procedure in order to establish the lawfulness of their processing operations. As stated in the press release issued by the DPA, Google declared that data were ñcollected mistakenly, have never been used for any service, have never been communicated to third parties and are currently stored on servers located in the USA [é]ò[55].
The DPA considered the data processing, in particular the collection of payload data, as potentially in breach of, *inter alia*, the section 617-quarter (1) and 617-quinquies of the Criminal Code, focused respectively on, ñwhoever fraudulently intercepts communications that relate to a computerised or IT system or else take place between several systems (é)is to be punishedò, and ñexcept where provided for by law, whoever installs equipment that is suitable for intercepting, preventing or discontinuing communications that relate to a computerised or IT system or else take place between several systems (é)is to be punishedò.
On the basis of the DPA evaluation, the case file was forwarded to judicial authorities. Additionally, the DPA ordered that Google Inc. stop, in pursuance of the Italian Data Protection Law, any collecting of Wi-Fi data.

As the authority received several complaints from Italian citizens about GSV, a decision was adopted in October 2010[56]. Under the Italian Data Protection law, in fact, data subjects have the right to: a) object to the processing of their data even if they can only be partially identified (e.g. Googleôs face blurring) and b) be informed of the processing. According to the DPA, ñthe arrangements for informing data subjects are insufficientò[57] and, therefore, the

[51] http://www.tagmenot.info
[52] http://www.tagmenot.info
[53] http://www.trailmeup.com
[54] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1751001
[55] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1751001
[56] http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1761443
[57] http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1761443.

authority took 4 actions, which included:

1. the appointment of a representative based in Italy in order to enforce the compliance with the Italian DPA;
2. adequate information (publishing 3 days in advance, on its website, the date of when image acquisition will start) to data subjects on the routes patrolled by Google cars;
3. adequate information to data subjects also through advertisements published in at least two local newspapers and broadcasted by a local radio.
4. Visible stickers on Google cars in order to make them noticeable.

Since 2010, articles in mainstream Italian media on GSV have been mainly focused on challenges faced by Google outside the national context, especially in the USA.

Google's Street View in Slovakia

Martin Kovaniļ

Google's Street View in Slovakia was at first (2007-2009) picked up by technological media, especially Internet sites, by explaining technology and the ecosystem of the project. Later coverage, again almost exclusively by technological media, focused on project launches in individual countries, covering problems of GSV project in Britain, Germany or Switzerland. As the GSV project moved to neighboring Czech Republic, where its first part was launched in October 2009, media reported about problems it was facing. Czech DPA criticized Google for not registering the GSV project, and temporarily refused to grant Google data retention permission, a conflict that continued all through 2010.

The actual GSV project in Slovakia started in 2010. At this stage, media coverage was influenced by a decision of Google to establish a regional office for Slovakia in December 2010. It is obvious from media analysis that the PR department of Slovak Google worked hard on presenting the GSV project for Slovak media in a most "friendly and accessible" way. All national media covered the announcement of the GSV project in Slovakia. Headlines included "*Slovakia Goes to Google*", "*StreetView also in Slovakia*"; "*Watch Out for Cars with Cameras!*".[58]

Later, media offered additional reports on the GSV project that also included news on problems of GSV in other countries. For example, the most popular Slovak daily, the tabloid Nový ļas, reported in August 2010 in an article entitled "*This is How You'll see Your House on Internet*", that the GSV project met with problems in several countries. "*Germans are protesting against GSV and Slovakia is calm.*" The article pointed out the problems of GSV in Germany, and stressed that GSV could be a useful tool for burglars in assessing future targets.[59]

In September 2010, media informed that GSV in Slovakia have not started yet, because the Slovak DPA was still negotiating with Google on conditions of the project. Despite early optimism, GSV in Slovakia started officially more than a year later than originally planned, in April 2012. According to the Slovak DPA, the delay of the project was not influenced by the registration process, in which Google, as in Czech Republic, promised to lower its cameras

[58] Slovensko ide na google, Plus jeden deŇ, 2010/08/12 ; GSV prichádza uģaj na Slovensko
Zdroj: SME, 2010/08/12; Pozor na autá s kamerou!, Nový ļas, 2010/08/13

[59] Nový ļas, Takto uvidíte váģdom na internete ("This is How You'll see Your House on Internet"), 17/08/2010, p. 14

from 2.7 to 2.3 meters, to automatically blur faces and car number plates, and to avoid recording material in rush hours and near localities such as schools and churches.[60]
Another important PR coup for Google was the establishment of official contact with Slovak authorities, both national and local. In February 2012[61], the Transportation Minister J. FigeĎ publicly supported the GSV project as a great tool for the propagation of Slovakia, the Slovak tourism industry and Slovak SMEs. Leadership of ZMOS, the biggest organization of Slovak Mayors, expressed the same enthusiastic support for the GSV project. The media, especially local media, were full of reports that informed about GSV decisions to photograph their respective city, or complained that their city was not included. This "goodwill" was picked up by Google, which revised its original plan for coverage and included more Slovak cities.[62]
The official launch of the Slovak part of GSV in October 2012 was reported in all media, followed by dozens of articles that asked people to provide embarrassing photos[63]. Only a few articles went further and pointed out unclear privacy issues about the GSV project.[64] No official complaints to the Slovak DPA were reported. The overall success of GSV in Slovakia and the unproblematic preparatory phase probably contributed to the decision to expand GSV. In a new project, which was announced by Google Slovakia in 2013, GSV will expand its coverage of Slovakia, also using GSV Trike. In addition, Google will work closely with governmental agencies in order to "revive local culture and traditions in Slovakia through online technology".[65]

Conclusion

It would take less than an hour for a Google Street View car to drive from the city centre of Vienna to Bratislava; nevertheless the case of Googleôs Street View is a very good example how national, legal, historical and cultural differences shape the public perception of technologies. The country reports in Annex I were conducted before the interviews took place to better understand how different national contexts should be considered in the analysis of the narratives in the following chapters. They display a number of national differences with regard to the attitudes entertained towards surveillance. The results from the country reports provide valuable background information for the detailed analysis of the stories elicited in the interviews. A systematic analysis of country-specific perceptions will be subject to further investigations beyond this project.

[60] See for example: Slovak Spectator, Google finally views Slovakia's streets,16/04/2012
[61] See: DSL.sk, Ministerstvo dopravy chce, aby Google na Slovensku spustil GSV (Ministry of Transportation wants Google to launch GSV, 14/02/2012
[62] See: Zive.sk, Googlu sa asi Slovensko páļi, bude fotiŠ Ņalģie mestá (Google probably likes Slovakia, To Photograph Additional Cities), 19/04/2012
[63] Several of them included photos from Roma settlements.
[64] See for example: Nový Ļas, 06/11/2012, Poruģuje Google naģe súkromie (Is Google Violating Our Privacy?); SME, 02/11/2012, Google odhalil naģe ulice aj chudobu (Google showed Our Streets, But Also Poverty), p. 5
[65] "Na slovensku notu", https://sites.google.com/site/slovenskanota/home .In a statement on opening page of the site, the local Google director ñthanked Slovakia and Slovaks for their hospitality and interestò.

2 1ST DILEMMA: PRIVACY AND CONVENIENCE

Daniel Fischer, Wolfgang Bonß, Nils Zurawski,

2.1 INTRODUCTION: CITIZENS AS CONSUMERS, PROVISION OF SERVICE IN MODERN TIMES

In this chapter we want to address the problems and dilemmas/trade-offs emerging in the world of electronic consumerism. While almost all forms of shopping and consumption could have been performed anonymously in pre-Internet times, this is no longer possible. One reason lies in the changing methods of payment and the problem of establishing trust in commercial relationships without cash transactions. Paying cash over the counter allows for highly anonymous transactions. By paying with cheques, credit cards or advanced forms of electronic payment like PayPal consumers have to identify themselves and hence leave data traces; by shopping via Internet they provide additional relevant marketing information about what they buy, when and where they shop and what they look at before and after buying. This may yield various data concerning, for instance geo locational information, personal preferences, medical conditions, personal relations and so forth. Using these data, profiles could be constructed in order to derive e.g. credit ratings from shopping patterns or postcode information.

What can be observed here is a paradox of anonymity. Being involved in a commercial transaction with your local shopkeeper may create a social relation, in which anonymity ceases to be an issue, and relations will be re-configured and once anonymous customers will be rendered loyal customers, of whom the shop owner is well informed regarding preferences and so forth. This is represented in the iconic figure of the grocer at the corner-shop acting as a communication hub for the neighbourhood. In this setting an individual as a customer is known to his/her local community, but anonymous outside this environment. The same person shopping in an inner-city department store would enter into another setting, one in which anonymity is still a leading faculty. Businesses in such a setting do not know their customers personally. They neither know their names, nor preferences. Anonymity is the default setting, and at the same time, a problem for the business striving to extend their base of loyal customers in terms of advertising, offers and service.

Developing sustainable customer relations following the ñtraditionalò model of personal/intimate relations between local shopkeepers and their customers requires extended efforts in this world of anonymous consumerism. Loyalty cards and bonus programs have proven to be an effective way to achieve this. Collecting clientsô personal information and linking this information with shopping habits, businesses try to lure customers to their premises. This approach demonstrates the problem of privacy and convenience in a nutshell: consumers (citizens, clients, customers) give away personal information in exchange for presumably preferential treatment and increased convenience. Signing up for a bonus program or applying for a loyalty card still requires an active decision on the part of the individual, whom in principal retains the choice to remain anonymous. Thus, there is no necessity to exchange personal information for special offers, treatments or discounts.

This has gradually changed since the proliferation of the Internet since the early 1990s and its

rapid expansion since 2000.[66] The emergence of Internet-based e-commerce affected shopping and consumption patterns in many different ways. They lost their territorial grip, creating more convenient and economical opportunities for customers to screen and select from a wide array of goods and services, presented as seductive offers in virtual space. However, the emergence of this new form of commerce ï this is important in the context of our study ï made data provision mandatory for customers.[67] Using electronically mediated forms of shopping or payment, consumers are tied into a comprehensive system of data collection. Connecting to the world of e-commerce requires repeated and continuous personal identification and creates a multitude of behavioural data, which puts these dimensions of current consumer practices at the heart of what we have defined as ñsurveillance societyò. In this context consumers cannot avoid being transformed into leaking data containers, continuously leaving traces of their daily actions and movements. Therefore, we wanted to analyse this development within four empirical settings: the use of loyalty cards (1.2), online shopping (1.3), the use of Internet (1.4), and misuse of personal data (1.5). Before we present our empirical findings, we would like to briefly introduce the settings that we have chosen as focal points of our analysis and how they build upon each other.

Loyalty Cards

Loyalty cards hold a prominent and special position within shopping practices. Loyalty to a store (known as customer loyalty in marketing terms) is an inherent part of modes of consumption since the advent of the department store, mass production and the consumer as a social figure from mid-19th century onwards. As consumption, particularly shopping has been widely affected and its forms changed or influenced by digitalisation, so have loyalty cards. They have become part of the global personal information economy.[68] This topic generates interesting stories, since the act of data production and collection requires activities on the side of the customer: a loyalty card has to be ordered, the application form has to be filled out with personal information, the card has to be handed over at the cash desk. So the act of data collection is clear for the customer to see and suggests an active involvement. Thus loyalty cards within the IRISS research were addressed in the course of the interviews and yielded interesting answers from which important evidence for further development of the concept of ñdoing privacyñ can be drawn.

According to a survey by Finnaccord[69] across Europe as a whole, loyalty cards achieve the highest usage with fuel retailers (88.5%), department store / variety retailers (34.0%) and supermarket / hypermarket chains (28.4%). Estimates on the amount of loyalty cards in circulation in Europe are difficult, but some examples may provide a small insight. About 85% of households in the UK have at least one loyalty card, according to the market researchers TNS. Tesco's Club Card is the giant, with 15 million active members in the UK alone.[70] The amount of users does appear to be falling though, or at least UK shoppers are

[66] Castells, Manuel, *The rise of the network society*, Blackwell, New York, 1996.
[67] Garfinkel, Simon, *Database Nation - The Death of Privacy in the 21st Century*, O'Reilly, Cambridge et al., 2000.
[68] cf. for example Zurawski, N., ñLocal practice and global data. Loyalty cards, social practices and consumer surveillanceñ, *Sociological Quarterly*, Vol. 52, No. 3, Fall 2011, pp. 509-527. Also: Pridmore, J., ñReflexive marketing: the cultural circuit of loyalty programsñ, *Identity in the Information Society (IDIS)*, No. 3, 2010, pp. 565-581. Also: Coll, S., ñConsumption as biopower: Governing bodies with loyalty cardsñ, *Journal of Consumer Culture*, Vol. 13, No. 3, 2013, pp. 201-220.
[69] http://www.finaccord.com/documents/rp_2013/report_prospectus_retailer_payment_gift_loyalty_cards_europe.pdf

[70] cf. Daily Mail, 25.06.2012: http://www.dailymail.co.uk/news/article-2164270/Loyalty-cards-25-million-shoppers-used-Government-snoop-eating-habits.html

using them less than they used to ï a drop of 8 million in active use has been reported.[71] In Germany the biggest player is *payback*, claiming that 60% of Germans hold a payback-loyalty card. Furthermore, it is estimated that every adult German holds between 2 and 4 loyalty cards of some sort. For the Italian market, estimates state that since the early 2000s, the biggest 20 distributors manage loyalty programs involving over one million registered customers with around 20 million active cards in all sectors.[72] In contrast in Slovakia, it is estimated that 90% of all customers are equipped with a card or are users of a program ï up from 69% in 2006[73].

Online Shopping

A fundamental shift in the constellation of advertising and shopping practices can be observed: Whilst consumers increasingly ñgo shoppingò online, they ñgo browsingò in shopping centres.[74] There, e.g. flagship stores offer the ultimate branding experience, while the actual purchase occurs later via the Internet. Online shopping, however, radicalises the principle of loyalty cards: Although consumers have to engage actively, e.g. by creating an account on *Amazon*, *EBay* etc., many other data are recorded automatically when visiting a companyós website: How much time was spend on a site? Which items were browsed or put into the shopping cart? Which other sites were visited before?[75] The customer no longer remains anonymous in online shopping, since every action/click is recorded, stored and analysed for marketing purposes. Although the benefits of online shopping are obvious for the consumer (perfect availability of goods, comparability of prices, convenient delivery, etc.), payment remains the one crucial aspect. However, there have been many developments in the payment services sector (such as PayPal, Amazon Payments, Credit Cards) and online banking, with ever increasing security standards preventing fraud and misuse of data. Part of our research in IRISS was focusing on the levels of awareness among users about these different ñpaymentò-acts and their implications: How aware are European citizens about online tracking? Do they worry about privacy infringements or are they more afraid of criminal misuse of data?

The importance of online shopping as a field of inquiry is highlighted by a few numbers. According to Ecommerce Europe (2013),[76] of 820 million people living in Europe, 529 million use the Internet and 250 million are e-shoppers ï almost a third of Europeós population (figures for 2012). Although the Internet economy only makes up for 3,5% of overall GDP in Europe, it nonetheless achieves 311.6 Billion Euro in Business to Consumer turnover.

Use of Internet

In the third field of analysis, we broaden our focus from the ñact of consumptionò towards

[71] cf. New Statesman, 21.06.2007, http://www.newstatesman.com/life-and-society/2007/06/tesco-supermarket-mother-data

[72] Cedrola, Elena, and Memmo, Sabrina: ñLoyalty marketing and loyalty cards: a study of the Italian marketñ,*International Journal of Retail & Distribution Management*, Vol. 38, No. 3, 2010, pp. 205-225.

[73] For more information in Slovak see: http://ekonomika.sme.sk/c/6461392/prieskum-vernostnu-kartu-vlastni-takmer-90-percent-slovakov.html

[74] Suau, Cristian, and Munar Bauzá, Margarita: ñThe mall in the online shopping eraò, Unpublished Paper, presented at the 4th International Conference of the International Forum on Urbanism (IFoU), 2009.

[75] For information on ñBehavioural Trackingñ see: https://www.eff.org/issues/online-behavioural-tracking; these data are so tempting that retailers try to build similar surveillance systems also for shopping centers: http://www.theguardian.com/technology/datablog/2014/jan/10/how-tracking-customers-in-store-will-soon-be-the-norm

[76] http://www.ecommerce-europe.eu/news/2013/10/eurostat-releases-figures-on-online-shopping-in-europe

general Internet usage (1.4), which can be described as a multitude of different services (communication, information, entertainment), which may appear to be Ăfor freeñ, but are financed via advertising that again is based solely on the production, collection, combination and evaluation of personal data.

According to the Digital Agenda Scoreboard 2012[77] of the European Union, ñFinding information about goods and servicesñ is the most used online service ï 71% of all users use search engines in order to find information, with Google the leading company used by approx. 80%. This is followed by ñReading and downloading online newspapers and newsñ, and Ăsearching for information on health, general knowledge (i.e. consulting wikis such as Wikipedia)ò.
ñSocial Mediaò and ñe-Commerceò make up for the second most important sector in Internet use. This ñtime spent on the Internetò is clearly recognized by the marketing industry, as online advertising grew 11.9% to a market value of ú27.3bn in 2013.[78] An *important trend that was addressed in IRISS is that Internet usage is decreasingly confined to the classical desktop/browser-based setting. Thus, the use of mobile devices makes up for 30% of daily internet usage in Europe, and here again more than 80% of the time is spent using* ***ñ****apps****ò*** *(messaging, shopping, social media, information) instead of browser based allocations. Such apps however collect large amounts of personal data. Most of this is performed by automated systems of data production, data collection and data evaluation.*
The percentage of individuals in the EU using the Internet in 2013 was 70%. About one third uses the Internet on mobile devices away from home or work. And 60% report use of the Internet on a daily basis. The level of Internet access ranges from 54% of households in Bulgaria to 95% in the Netherlands, which accounts for other more specified uses as well. It has to be added that by 2012 around 120 million European citizens have never used the Internet. Romania, Bulgaria, Greece, Cyprus and Portugal have the highest rates of non-users and account for 25 million citizens who lead their lives without the Internet (a figure similar only to Italy with 23 million non-users). Without going into a more detailed analysis of the statistical evidence it should be clear that Internet usage, whether at home, at work or on mobile devices is spread widely across most European countries, and the electronic services provided through this medium have become an elementary part of social, cultural and economic life in Europe. Table 1.1 shows detailed information for the countries participating in IRISS[79]:

	Austria	Germany	Italy	Slovakia	UK
Internet access (pct. of population)	81	83	58	80	87
Mobile Internet Access (pct. of population)	71	58	16	38	63
Time spent online via stationary/mobile device (hrs/d)	-	3.7/1.6	4.7/2,2	-	4.1/1.6

Table: Internet Usage in Europe /Countries involved in WP4.2

[77] cf. European Commission, Digital Agenda Scoreboard 2012 http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/scoreboard_life_online.pdf [pp.11-12]
[78] http://www.iabeurope.eu/news/european-online-advertising-market-records-new-high-273bn
[79] cf. European Commission, Digital Agenda Scoreboard 2013, Brussels, 12.06.2013.: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DAE%20SCOREBOARD%202013%20-%20SWD%202013%20217%20FINAL.pdf [pp.76-80]

Comparing these figures to the correspondent European average, shows that our interviews were conducted in countries with high internet penetration (except for Italy, all countries lie above the average of 70%). Concerning mobile Internet access, the European average is 36%, but in all countries the increase of online activities on mobile devices is considerably higher than on stationary devices.

Misuse of personal data, victim experiences in the digital age

The final section will focus on experiences of fraud and misuse of personal data, gathering narratives about how negative trade-offs are perceived and reconciled with on-going practices of (online) consumption, internet usage and the production of personal data this entails.

While detailed evidence of users is readily available it is difficult to assess the level of misuse or Internet-related crimes (e.g. identity theft, fraud, etc.). The Fraud Prevention Expert Group of the EU (DG Internal Market and Services)[80] states in its report on the matter that actual estimates are difficult due to the piecemeal nature of the data in the EU. However, the group estimates that in the UK alone 100,000 individuals are subject to identity fraud each year costing the UK economy roughly 1,7 billion Euros annually.

2.2 NARRATIVES OF LOYALTY CARDS USAGE AND THE ROLE OF ñPRIVACY MANAGEMENTò

2.2.1 Loyalty cards as ñbearable nuisanceò

We identified a number of different narratives about loyalty cards in our interviews. Besides a straightforward refusal of the cards ï mostly on the grounds of objections against limitless data collections and the ensuing dangers ï loyalty cards are met with what can be described as a practical scepticism, prototypically summed up in the following quote (answering to the question: Why donôt you like loyalty cards?):

> ***ñ****You leave your traces everywhere, and then they also sell your data. This happens and we know it. You get all of a sudden spam mails, as soon as you enter your e-mail address, or you get personal advertisement in your mail. [****é*** *] Itôs nothing evil, but itôs unpleasant.****ò***
>
> (Interview ID 499, 67 years, male, Austria)

It is not considered as an outright evil, but as a bearable nuisance that, following a recurring argument, either has to be considered as a trade-off in a digitalised world, but more often then not is accepted as an inevitable part of everyday life. It is interesting to note that very few of the interview partners had either no opinion on the subject, even if not owning or using loyalty cards, or did not know about it. There are varying degrees at which loyalty cards are rated ï from Äbeing a good thingñ to an outright suspicion of continuous malpractice concerning the collected data. This connects with a general feeling of mistrust that runs through many of the accounts. Such mistrust reflects the confusing situation of data collection and the conditions of digital everyday life in general. It reflects a constellation where an

[80] http://ec.europa.eu/internal_market/fpeg/index_en.htm;
https://www.europol.europa.eu/sites/default/files/publications/1public_full_20_sept.pdf

individual is exposed to an undefined, not identifiable, invisible, but nonetheless existing actor. All our respondents were convinced that something was happening with their data, but they had no operational idea, who was doing what. This created an almost Kafka-like situation of uncertainty: Ego (the card bearer) cannot see what Alter (the card issuing company) is doing but nonetheless knows that his actions produce some reaction on the other side. This uncertainty can be compensated by generalised trust, assuming the other side will act within the limits of law. But often mistrust seemed to be the default attitude towards these schemes. However this sort of mistrust does not automatically lead to open resistance or protest, but is often rationalised and woven in with further arguments addressing the personal use of loyalty cards. What becomes clear is that a vague awareness of the implications of loyalty cards exists, which seems to be provoked in the instances of talking about, but not necessarily when using them. Also, the reflections on the personal uses express this quite distinctively.

One would expect to find a clear distinction between what could be called positive or negative accounts. However although positive or negative statements do occur as such, many of them are ambivalent ï aside from responses that state an outright refusal, which are overtly negative. But also positive statements may display an ambivalent element, i.e. loyalty cards may be perceived as positive regarding the promised bonuses or discounts, while the same person may be suspicious when it comes to the collection of data. This again displays the double character of loyalty cards, as both a medium embedded in the mundane activity of shopping and a means to collect data for a global economy that takes a leading role in the process of producing glass consumers, a process eluding the control of the customers themselves. Hence an overview of positive or negative arguments also has to be grouped according to the addressed qualities of the loyalty cards and their setting. But it has to be noted that most accounts display the strong ambivalence of this medium as being part of everyday life through its use in shopping practices and as a data-gathering instrument, evoking discourses of surveillance.

2.2.2 Exchanges, personal data and privacy labour

Positive arguments for using loyalty cards circle around the bonuses, discounts, possible advantages and the argument to actually save money by using them, because some of the data is used for ***Ă****your own good****ñ*** (Interview ID 242). Some respondents argue that the other side (the card issuing company) obviously displays an interest in their personal desires and wishes, thereby adapting the situation to a person-to-person situation.

Not outright positive, but rather accepting the fact that loyalty cards are part of what shopping is also about, many arguments that stress the fact that loyalty cards are part of everyday life and always have been can be found, albeit in different forms and under different conditions. Some statements refer to stamp cards or sticky points that could be collected in the old days. They do not see a big difference in relation to customer loyalty or shopping practices. Here the loyalty part is emphasised, while the data collection aspects of the card are ignored.

However some statements hint at the fact that digitalisation has brought about changes in the ways advertising is targeting people, which is mostly felt as a nuisance, but not as threatening individual privacy. Shopping, it seems, is nothing that people, who have a positive attitude towards loyalty cards, view as something that should be necessarily being treated as a

personal secret. We would argue that this has to do with the integration of loyalty cards into shopping and hence into the rather mundane activities of everyday life.
Negative statements about loyalty cards (which were not necessarily produced by respondents who did not own such cards) were concerned mainly with the effects of targeted marketing, i.e. soliciting unwanted advertising to their mailboxes or phones via SMS. This was considered as an infringement on the right to freely choose what to consume (often framed as Ä*manipulation*ñ) on the one hand, and on the other the respondents felt unease at being rated, categorised and profiled by the company. The customisation of consumers to meet market needs was rejected. It was seen as an attack on the autonomy of the consumer, who as free citizen wants to choose without being manipulated by targeted offers.
Data protection is also an important issue when rejecting loyalty cards or making critical statements. Especially the selling of collected data to third parties was a high-ranking issue among interview partners and thus referring back to the issue of advertising and targeted marketing. Loyalty cardsó position at the intersection of everyday life, data collection and privacy issues as well as its prominence and pervasiveness often give it a special role, one that cannot be explained by its connection to the personal information economy alone. The following quote exemplifies this particular role and also highlights the role of Ăprivacy managementñ when dealing with personal information:

> ***ñI'm** aware of the privacy issues, although I am not really very active when it comes to privacy protection in the online environment. But when it comes to consumer loyalty cards, I do not use them at all. I know that they offer you some advantages, but I wouldn't use it, since I consider it too much of a privacy breach.**ñ***
>
> (Interview ID 601, 29 years, male, Slovakia)

Here a general lack of activity in dealing with privacy issues is confessed, when on the other hand the rejection of loyalty cards is clearly stated, because of the perception of a privacy breach. Privacy is managed according to context, technology used and personal reasons that are not further explained, despite the awareness of possible advantages for the consumer. So although this clearly is an exemplary account of rejection, it also displays the existing ambivalence towards loyalty cards. Furthermore, no matter whether positive or negative, many accounts display this ambivalence, in which Ăprivacy labourñ surfaces. Other statements show that there is awareness of the data protection and privacy issues that may be negatively connected with loyalty cards, but that they are used anyway. A narrative, which featured in many interviews, is that customers are Ăcomplicitñ in the gathering and subsequent processing of data. Although many things are not needed, they come in handy, and people are being Ăpracticalñ (Interview ID 232) about it. Again this supports the argument of privacy management or labour. The following quote serves as a very good example summing up the major aspects of the construction of the average narrative ï including awareness of data protection issues, a feeling of futility to resistance because of complexity, privacy management/labour and its role in everyday life.

> ***ñ**Of course: The companies know a lot about me, the whole mobile phone surveillance, they know everything about me. But what choice do I have? Not acting online anymore, just paying cash again? I think it's an all or nothing thing. Either you accept that and act like you wish or you do nothing at all. But to create some little*

nuances: No credit cards, but payback, or payback only at gas stations but not in the department store. Surf the Internet via special proxies but having an iPhone. I think that'sé no, much too time consuming and complex.ò

(Interview ID 303, 60 years, male, Germany)

The core of the dilemma of being a consumer in a digitalised environment of consumption is summed by the following quote:

ÄI have loyalty cards, yes. And I know that they also look at my data, what I buy and when I buy it, but thatôs ok for me, because I get my stuff cheaper. So I sell them my data, so to say.ò

(Interview ID 550, 34 years, female, Austria)

Loyalty cards on a very basic level offer deals within modes of consumption that are shaping citizenôs everyday lives. Given the complexity of a world that is deeply entangled with, if not almost exclusively dependent on various forms of digital data processing, there seems to be no other way than to surrender to data collections and data processing, as exemplified in the following quote:

ñWell, not engaging with any of those things, but itôs kind of hard to do that nowadays, ... Yes, youôd have to live on a farm in the middle of nowhere, grow all your own food, not use the Internet, because even things like ... because in order to buy a house you need a credit history.ò

(Interview ID 86, 42 years, female, UK)

To understand loyalty cards as a form of surveillance, analytical limitations regarding the term surveillance have to be considered, since it is used for quite different forms of protocolling, watching, monitoring and recording data or behaviour. In the case of loyalty cards there are certain problems. Surveillance was rarely evoked in the interviews in relation to loyalty cards. Thus, the perception of data collection, targeted marketing or consumer profiling is not linked to surveillance, in the same way as e.g. to NSA practices or state oriented snooping are. Although a major narrative highlights the trade-off or deal-narrative, this cannot be compared to the deal an ostensible benevolent state may offer its citizens, i.e. surveillance under the guise of security or the like. Loyalty cards are a part of everyday life, embedded in everyday activities and not perceived as something external to it.

So, if there is an awareness of the complexity of global data processing and also of the futility of resisting, one might ask why this does not lead to a shock, to a standstill or to open forms of resistance. Open resistance in a consumer society, one may argue, is only possible within the realm of the consumer society itself, i.e. not by its denial. Hence resistance is achieved through measures of privacy labour. Thus privacy labour is the key to understanding societal resilience in terms of data collection. Making sense of the trade-dilemma, the consumer/citizen "ignoresò or ñsurrendersò in order to reduce complexity. The situation is simply not bad enough to be socially disturbing, and consumption is part of everyday life and vice versa. Consumption is not repressive (or not felt in that way), which makes it more difficult to evade its ostensible necessities, such as giving personal data for services enjoyed.

ñThe distrust that has grown over decades not to become too transparent thatôs it in

the end é . I must say, my wife has loyalty cards of course, then again it is my wife who goes shopping and not myself. My wife has all of them, Merkur, Billa, whatever é There is certainly a certain distrust. It is probably also an age issue. One has experienced another time. One knows surveillance states etc. So I do not want to become too transparent. You can only avoid it to a certain extent. You cannot travel and pay everything in cash, you cannot avoid using debit cards and credit cards.ò

(Interview ID 40, 55 years, male, Austria)

In effect the use of loyalty cards reveals strategies of privacy management and a very clear and at the same time futile outlook on the digital world. Differences can be observed when comparing ñlay citizensò *(digitally naïve*) and ñdigital expertsò (*digiterati*). People identifying themselves as experts (or who are put into that category by e.g. their job description), show a somewhat more self-confident mode of handling loyalty cards and dealing with the problems connected to their use. They seem to know more and also mention a certain knowledge that enables them to assess the risks and engage in somewhat more informed privacy management. They are not worried, they pay attention and have developed quite sophisticated routines, as for instance multiple email accounts to circumvent being a totally transparent glass consumer. Resilience here seems to be connected to a form of risk management by knowledge, not withstanding the fact that these experts do not necessarily reject loyalty cards by default, but also embrace the advantages, while at the same time claiming to know how to handle the complexity.

2.3 ONLINE SHOPPING

As pointed out at the beginning of this section, the B2C sector of electronic commerce has witnessed a crucial expansion: Shopping activities and advertising practices are no longer bound to limits of time and space, but goods can be advertised and consumed/ purchased anytime and anywhere. While the positive aspects ï i.e. enhanced convenience through increased availability of goods, competitive prices and bargains, and instant home delivery ï are appreciated by a majority of respondents, the negative aspects are perceived and appraised differently.

2.3.1 The daily loop

A few respondents mentioned advertising as a concern. They considered advertisements to be redundant, cloddy, or classified them as Ăjunkñ. The following accounts identify typical problems or unease with the proliferation of advertising through emails that were casually provided in seemingly harmless circumstances:

ñYes last time I was looking for boots at an online shoe shop. Now there is always this ad for a certain brand of shoes on my Facebook profile. I donât like this but what should you do? I donât really pay any attention to advertisements to be honest.ñ

(Interview ID 521, 21 years, female, Austria)

ñPersonally, I just think this is done in such a primitive way. I search for "guitar XY",

they show me: Here's guitar XY for the cheapest price. I mean come on... I think other people, especially young people also know that. Because that's pretty much a topic, yes.ñ

(Interview ID 201, 21 years, female, Germany)

The majority of our interview partners understood this particular business model that is based on advertising. Nevertheless, they consider advertisements as an inconvenience and annoying, and an additional cost of their shopping activities. The act of shopping does not end with the actual purchase of an item, but consequently is further deepening the relationship between company and customer. As a result a continuous flow of advertisements is forced upon the consumer ï seemingly in return for its loyalty. However this does not seem to be sufficient to create open resistance against such practices:

ñI don't like that personalised advertising. I always see the same. It's not torturing or really on my mind all the time, but if there was an initiative against that, they'd have my signature.ò

(Interview ID 198, 21 years, female, Germany)

2.3.2 The glassy customer

A common form of advertising is to offer things that have been bought or looked at before. Advertisements follow a motto of ñsame, same, but differentò ï e.g. guitars are offered to guitar players, hotel vouchers to regular travellers and so forth. Another strategy is to analyse the collection of increasingly complex personal data by one or more companies over time, i.e. profiles of behaviours, preferences and locational data. The goal is not to satisfy recurrent needs that can be deduced from specific shopping or online histories (by way of cookies or else), but to distil a more encompassing profile of a customer based on a multitude of direct and indirect information. When this takes place in an everyday life setting such as shopping activities ï e.g. in a supermarket ï it creates multi-layered, rather emotional reactions on behalf of the consumer/citizen:

ñIt has put me off; it has actually put me off. And Iôm even a bit like that with the bloody [supermarket] website because it brings up all your list, and you know how. which is really irritating... after youôve finished your shopping it then asks you if you want all these things because youôve ordered them before, and itôs a complete con and I feel like Iôm being conned all the time, theyôre trying to just get me to spend that little bit extra, and so I never click on any of those things and, in fact, it makes me not want to order through [supermarket]. I think that sometimes... because itôs also useful because itôs useful to have your list up there that youôve already ordered and itôs useful to remind yourself that youôve ordered all those things, but I think they have to be really careful about the balance ... and I think thatôs the thing, itôs actually quite useful for companies to remember all your information, and itôs actually quite nice, like with your loyalty card thing, that you might get adverts through about certain things that might be useful to you and you might not notice otherwise, but I think it is a bit too much sometimes.ñ

(Interview ID 82, 42 years, female, UK)

Quite clearly we can observe a psychological process within which the respondent is balancing chances and costs, commencing with an emotional reaction towards the non-stop, penetrating efforts of businesses to make people buy more. A first reaction is total denial *(ÄI never click on any of those things.ñ*), which then resolves into a more rational assessment of the situation. Itôs interesting to note that the respondent doesnôt differentiate between being reminded of buying things already bought and being offered things that she *Ämight not have noticed otherwiseñ*. This particular respondent is a good example of someone who hasnôt found a good balance between denial and appreciation of the loyalty programs sheôs offered or takes part in. Such an account represents an exception, since most people show a more or less relaxed way of coping with the ñnew waysò in which they are treated and targeted as customers:

> *ñIt seems like itôs hard to avoid someone building up a picture of who we are, obviously figure out weôve got kids and la, la, la. Yes I donôt like it, I donôt particularly like it but Iôm not horrified by it.ñ*
>
> (Interview ID 71, 35 years, male, UK)

> *ñNo, I havenôt had any experience with misuse of personal data, really. No. I suppose weôre getting onto this, but I just accept that thereôs no privacy.... You canôt be King Canute and hold back the tide, is, I suppose, what I think. Well it is a deal, isnôt it? If the market is transparent, the customer has to be as well who wants to use all the data.ò*
>
> (Interview ID 131, 69 years, female, UK)

Respondents claim that they are fully aware of how much information is collected about them. Denial and open resistance are not viewed as preferred, and indeed promising, ways to deal with this situation. Our findings suggest that increased knowledge about the complexity of data flows in the commercial sector doesnôt result in more caution concerning online activities:

> *ñI have credit cards, yes, and I have all kinds of loyalty cards, although I have informed myself now on what happens with the collected data, how they link them and the like. I am not sure anymore whether I really want that everywhere ... but my data is already spread out.ò*
>
> (Interview ID 172, 63 years, female, Austria)

> *ñAnd Iôm also aware that Amazon stores the data and has profiles for every user. They also sent e-mails with ówe recommend you this and thatô and that always matches very well with the things I previously bought. But thatôs the price you pay for shopping there, which is of course very convenient.ñ*
>
> (Interview ID 477, 32 years, male, Austria)

> *ñConcerning companies like Amazon, EBay or PayPal, there I have no scruples. What does Amazon know about me? They know my name, my address, my credit card and my shopping preferences, because I shop there. And those are things where I think that they need them, to do their job, to offer me products, to send it to me and to bill*

them. Itôs not disproportionate.ò

(Interview ID 494, 32 years, male, Austria)

People display a readiness to give up privacy in such settings, as long as they can see a clear benefit (special offers, good prices) for themselves, and as long as this benefit outweighs any annoying side effects (advertisements, etc.) that accompany it. Strangely enough, the same service is considered an infringement and is dismissed when other people find out about their purchases or preferences, as a result of their collection by Amazon.

ñYes, what Amazon is suggesting to me that I should buy next, is most of the time actually something Iôm really interested in. Except for the kidsô toys Iôve bought for my grandson, there they are wrong with their suggestions but for music and books they have quite a good instinct. What I did was that I enabled the privacy settings for my Amazon account. That is something a former student of mine taught me years ago. She showed us how you can figure out what kind of books the former Austrian President had bought with his Amazon account. I donôt want that. I donôt want them to know what Iôm buying. That is something nobody should be interested in.ò

(Interview ID 292, 72 years, female, Austria)

In conclusion, our findings show that the narrative of the Ăglassy customerñ is made up of three elements: First, there is a reflex to hide information, due to the feeling of being trapped and overwhelmed by the permanent efforts of companies to identify the needs of their customers. This results in more emotional utterances. Second, there is a more relaxed, but not more cautious handling, of the situation, often emerging from an increased knowledge about data handling practices by companies. Third, it is obvious that transparency exists only as transparency of the consumer, rendering the assumed trade-off a one-sided one, while there is little to no transparency on the side of corporations or businesses, for instances in terms of data usage, data deletion or data processing.[81]

2.3.3 Itôs the money, stupid!

So far we have learned much about our respondentsô instincts regarding privacy infringements that occur while shopping online. This last section draws attention to a more mundane and indeed widespread phenomenon concerning online shopping: The fear of becoming a victim of fraud as the following quote illustrates:

ñ[...] I guess Iôm not sure what I would be worried about in terms of somebody using my passport number because if somebody pretends to be using my passport number Iôm not sure what they can do and would it harm me. For me, the biggest fear would be... thereôs two big fears, one of them is anything to do with my children, and the other thing is money, them taking my money. But in terms of, I donôt know, some

[81] We see this as an important point considering some arguments being used by data protection activists: Often they illustrate the NSA practices by asking people to send them an email with all their passwords to Facebook, Ebay, Amazon and the likes, which of course nobody would do. But these are two different things in the eyes of the people: Being exposed to an anonymous institution is something different than being exposed to a specific person, who is in any way known or even stands in any kind of relation to you.

criminal somewhere pretending to be me, as long as itôs not impacting on me I canôt... and thatôs probably a crazy way to view it, but, yes.ñ

(Interview ID 859, 42 years, female, UK)

The experiences expressed in the interviews provided a wide range of cases. Regarding credit cards, respondents emphasised the good experiences, particularly when problems occurred. The conclusion was that credit card companies themselves were under public surveillance and wouldnôt want to risk having a bad image:

ñI shop online quite a lot. I never had a bad experience. When I shop through e-bay, it happened a few times that some damaged goods came or I did not get them, I wrote them and I got the money back. I even took advantage of this a few times, I got the product and I wrote them that it did not come and I got the money back. I think that they donôt want to risk bad reviews so itôs easier for them to send back 20 euro. I never order anything too expensive.ò

(Interview ID 774, 25 years, female, Slovakia)

Only few respondents claimed to avoid online transactions completely, without being able to state clear reasons for this. They argued that it would be more of Ăa feeling thingñ, Ămysteriousñ or would call themselves Ăphobicñ.[82] However, most followed clear principles or rules to put self-induced limits on their activities:

- only paying via third party companies, that offer insurance (PayPal, prepaid-Credit Cards)
- only buying a particular set of goods or services online (vacations, train tickets, books, records) ï things they cannot get otherwise, products under 100 Euro
- only performing online shopping from home, not via public or semi-public WIFI Networks

The theoretical concept of the ñtrade-offò which we employed in our analysis seems to be quite valuable in these cases, as every piece of information given away, is presumably resulting in a service returned ñfor freeò. However, the permanent presence of advertisements and shopping options is perceived as stressful, if not annoying, which in turn may result in some form of fatigue or carelessness, ultimately with serious consequences:

ñKeyword Amazon, yes I admit I got very lazy through time. I order a hell of a lot of my books there. It is so easy, practical and convenient. And I donôt care too much about the profiling, I bet I have some sort of ōinto special posh weird pop cultural stuffó.- profile, I can surely live with.ñ

(Interview ID 992, 44 years, male, Austria)

[82] "Somehow I feel I do not have a control over my credit card, I prefer brick stores.ò Q: ñBut if it is the same store you use, even in that case you will not use its online version?ò A: "No, I wouldn't, I would go there in person. I am almost phobic when it comes to online banking. I dont do it, well yes, but not very often. Itôs more of a feeling I have. I find this mysterious, I dont know so many things, giving my credit card details, and PayPl, I dont know how that works. It is not really my thing to shop online.ñ

2.4 USE OF THE INTERNET

From the dilemmas described in the previous sections, multiple connections between everyday life activities and online services emerge. These connections may be exploited to pursue political as well as economic interests, which in turn may analytically be classified as privacy infringements, e.g. in a juridical sense. But how are the same infringements identified by people on the streets? Are they also viewed as infringements into their own privacy? We have analysed three accounts along which we can describe how people perceive this dilemma and react accordingly.

2.4.1 The ĂDead Endñ-story: Pervasive, ubiquitous, useful, inclusive

> ***ñ****I don't think it is possible to protect your personal data from being accessible and being public. If I wanted to have my data protected, I couldn't exist...****ò***
>
> (Interview ID 413, 22 years, female, Slovakia)

> ***ñ****You are dependent on the technology. I couldn't imagine that you can for example study nowadays without Internet. ... Nowadays, you simply need all the folderol. That makes it easier for people to trace you.****ò***
>
> (Interview ID 158, 28 years, male, Austria)

A considerable number of statements in our interviews hint at the fact that people think of online surveillance as inevitable. Describing the situation as an Ăall or nothingñ option is regularly the starting point of their accounts. Thereafter, the handling of the situation differs: Most people emphasise the positive aspects of the trade off, since Ăbeing abstinentñ or cancelling the trade-off is considered impossible:

> ***ñ****The convenience I gain by using dropbox and similar services, outweighs the risk of being harmed, because I suppose that if he means to do it, it will happen anyway.****ò***
>
> (Interview ID 486, 32 years, male, Austria)

Another important element of how people perceive the situation is that privacy and security are often used interchangeably: You cannot achieve total security, neither for yourself, nor for your data. So that leads to a reflection of how to balance interests for privacy needs and convenience, which eventually cannot be resolved:

> ***ñ****Yes. It's funny. I'm aware of how vulnerable your own networks are but I suspect, like a lot of people, I suffer from security fatigue. When I set my passwords I'm slightly idle. When I've put a password in and they said moderate security and I've tried various permutations and it's still moderate, I can't be asked to find one which says high-level. Which is ridiculous, really, because I'd like to think I'm reasonably well-versed in the threats out there. But, again, it's a kind of security fatigue. It's just like there are so many passwords for this and that and after a while you just feel like well, I've got to get on with life, I can't...****ò***
>
> (Interview ID 36, 27 years, female, Italy)

Here the notion of privacy-as-security emerges and it seems like an associative reflex, which is somehow positioned in the cultural understanding of privacy. Ultimately this is a dead end, since Ătotal securityñ is a condition that is deemed un-accomplishable.[83]

> *ñYou would more or less need to give up your wealth if you really é But that is actually quite paranoid, if you are so annoyed by that, then you give up everything, no internet (é) you would go to an internet café to look up the various things that interest you. You would live simply, like in former times. If you want to write a letter to somebody, you would actually write a letter by hand and bring it to the post office é because Internet é I have seen the worst documentaries. Everything that runs via Internet is known by people. There is no way that you can protect yourself well enough.ò*
>
> (Interview ID 151, 28 years, male, Austria)

2.4.2 Privacy Management

Having realised both the inevitability of online surveillance as well as the positive aspects that come along with it, people start managing their privacy in a very complex way, i.e. as something that could be described as a form of *cognitive coping*. Itôs important for people to assume, that although their personal data are being collected, they are not the target of surveillance activities as an individual:

> *ñSo, like I said, because if you wanted to assemble all the information thatôs ever been on the internet about me you probably could, but I think it would take a huge amount of effort and I wouldnôt imagine you would do that, like that any... I donôt think that a couple of guys who want to defraud me and take over my bank account would go to that extent, so Iôm not really so worried about that and the CCTV footage of me walking into a shop.ò*
>
> (Interview ID 143, 18 years, female, UK)

> *ñAlthough I think that they store a huge amount of data about citizens, but they can never analyse all the data. I know that technically, it's possible and I think it is done, but I don't think that MY data is analysed.ñ*
>
> (Interview ID 480, 32 years, female, Austria)

This response clearly illustrates a position, which assumes that mass surveillance is not directed against specific individuals. Many accounts reflect on the complexity of mass surveillance, which is seen rather as an appeasing fact than as a genuine source of danger, in contrast to strategies that depend on a certain level of criminal energy:

> ñ*I am not interesting enough, to have my data exploited in the large mass, for that Iôm not a thrilling target. If someone means to get my data, or to sabotage my PC or*

[83] We believe that the understanding of privacy in terms of security concepts should be discussed and criticized. Privacy functions as a value that is generated by securing the absence of harms. Thus, we never found anything that could be interpreted as a Ăpositive concept of privacyñ in our interviews. We assume that this is due to a structural change of the concept of privacy over the last decades.

whatever, then he will succeed. If someone really tries, then it doesn't really matter what I do.'

(Interview ID 486, 32 years, male, Austria)

2.4.3 Symbolic resistance

Besides strategies of organising knowledge about surveillance along specific elements or categories, we identified quite a few symbolic actions used to emphasise awareness about online surveillance. In fact, it is quite rare that people do not regulate or limit their online activities at all. The common objective is to minimise connections between the "online' and the 'real' identity. This is achieved by the following actions:

- avoiding pictures, where someone is clearly recognisable
- eliminating the full/real name from online platforms
- having a 'registration' email-address that is not used to communicate with others and only known to the individual.
- turning off GPS-systems within all applications, if this is not required for the very sense of the application (e.g. in navigation systems).

We found differences in terms of how well informed people were about the effectiveness of their measures: Some interviewees knew that these measures could be thwarted by the actions of others (who may identify – i.e. tag – people on their own pictures or give away similar information):

'A friend of mine showed me, that even if I am not on Facebook, she can insert my name when she's "checking in" somewhere. Or that she can identify me on pictures with my name and so on. Or that she can see where somebody is at the moment.'

(Interview ID 70, 55 years, female, Germany)

We classify these strategies as 'symbolic resistance', although we cannot generally tell whether people really know how effective such measures are. It seems that these actions are directed against threats, which are expected to emerge in peer-to-peer interactions. The ability of algorithms and intelligent software to track a person is often not perceived as too problematic, as long as these efforts are directed against masses of people. However, it is seen as problematic, if one can be traced by ordinary people, simply based on one or very few pieces of information known to someone else. And in the case of social media, users are urged to provide a plethora of data through which a more or less complete identity can be reconstructed. Additionally, it is not only the company itself, which is aware of this information, but also individual users, i.e. when they are 'a contact'.

'I am always asked to 'accept' that, x and y said that I am attending this university, that I have attended that school, or that I am a member of this sports club or something. Which is true of course, but I don't want to be found via this information.'

(Interview ID 1001, 21 years, female, Germany)

Respondents choose a variety of strategies, to share information and personal data on the Internet or online storage (i.e. clouds). Some respondents share or store *'as little as*

*possible*ò, others share/store only ñ*the most important*ò things and others again, share/store only unimportant documents. However, most find it reasonable to think about the issue, even if it leads to ironic or sarcastic comments regarding oneôs own carelessness.

> ñ*I try to avoid sharing too much of my private data online, in that respect I donôt really like online platforms and apps. But my passwords (laughs) arenôt that safe on the other hand. I always use the same password for every platform I visit. One shouldnôt do that but I canôt remember dozens of different passwords.*ò
>
> (Interview ID 460, 34 years, male, Austria)

2.5 MISUSE OF PERSONAL DATA, VICTIM EXPERIENCE IN THE DIGITAL AGE

Reactions to the misuse of personal data, i.e. the experience of being a victim Ăin the digital worldñ follow on from narratives on the uses of loyalty cards, online shopping or assessments of internet usage as such. Quite astonishingly, quite a number of our interview partners had experienced data misuse, identity fraud or skimming attacks on their email accounts, credit cards or elsewhere. A main thread that runs through the accounts of misuse experiences is the aspect of complexity of the online world, i.e. a certain futility vis-a-vis the digital environment that has evolved into a fact of everyday life in many aspects ï ñ*actually, you canôt succeed in leaving no traces world wide. (é .) (Interview ID 60).* However, privacy management does also play a major role in many of the accounts we have gathered. Some respondents are very savvy and aware, mostly those identifying themselves as experts in the field, often persons that work in the IT sector ï they take serious precautions to protect their data, knowing about the technologies, the procedures and their often incomprehensible nature as well as the dangers lurking behind them.

> ñ*I donôt use them because I experienced a misuse with my data ï identity theft ï and I also protect my personal data. Windows shouldnôt be used because there are many security bugs. As an activist, I do have something to hide in my computer so I use a tool, a virtual machine, to surf the web. What I do on the Internet cannot be tracked and I use TOR. I always encrypt my emails and Iôve always encrypted all my communication. Cryptography is nothing strange, it is a forma mentis. 50% of my friends use encrypted emails and we also use other ways to communicate, for instance VoIP. Weôre developing specific tools to communicate.*ò
>
> (Interview ID 19, 26 years, male, Italy)

The following quote shows how the difficulties to fully understand how data protection works, what it actually implies and the futility of being able to protect oneself is rationalised. This quote is an example of a more general trend.

> ñ*I recently got to know an expert on data protection, at a seminar at my company. But what she does exactly*é *I must confess, I don't know*é *haha. But when I see and hear, that even big companies are not capable of protecting their data properly, how should I do this as a small company or as a private person?*ñ
>
> (Interview ID 360, 69 years, female, Austria)

Being personally confronted with misuse of data or other forms of fraud and theft the interviewees reveal a high degree of competence in dealing with these issues, often personally or by involving police, data protection offices or consumer advocacy groups. The following account tells of an often surprisingly relaxed reaction to incidents of hacking, data theft or else.

> *ñI have been a victim of hacking, it happened twice. The first time it happened 7/8 years ago, I reported it to the Postal and Telecommunication Police, as I contacted the call centre of my account and they suggested I report it to the police. [.....] Anyhow the police solved this situation within 3 weeks. Yesterday afternoon it happened again: Gmail asked me if I tried to access my account from China. I contacted the police to report an attempt of hacking. At the end the police just informed me that the provider cancelled my account and suggested I create a brand new account.ñ*
>
> (Interview ID 103, 28 years, male, Austria)

In other cases, such as credit card theft and misuse of data, people seem to know where to call, what to do and where to do it and showed a high degree of trust in the system that helped them to rebuild their digital lives. The problem here is that the misuse of data is quite diversified and refers to a multitude of incidents ï among them data theft, selling of data by companies to generate money, the use of existing data by intelligence services such as the NSA in their quest for terrorists, especially if it concerns presumably deleted data from old email, *Myspace* or *Facebook* accounts. Fraud and misuse seem to be perceived as inherent facts of life in the digital age as one Ă*canâ t succeed in leaving no traces world wideñ (Interview ID 60).* Although the misuse of oneós data implies being a victim of a crime, reactions differ from reactions within narratives that address crime prevention measures, most often relating to urban or public security. In contrast, within these cases calls for more police, stronger measures or prevention were articulated, whilst in the case of data misuse in general, the reactions displayed a form of resignation, due to misuse being ópart of the dealô of online (inter)action. This is not to say that respondents did not feel pain or loss accordingly, but the interviews suggest that this is dealt with on another level and more in line with other narratives on the digital and the role of data and privacy management. The following quote exemplifies this reaction or narrative:

> *ñI had a bad experience with one website that used a registration process as a valid contract agreement, and if you agreed with the terms, then they send you notice, with the invoice by post that you have to pay for visiting their site. It contained my address, but not my real name, they used the nickname I registered with on the site. I contacted the Slovak Trade Inspection, they recommended one consumers' association, and they, together with media solved the problem after a while. I paid nothing to the company. Around 2000 people had this problem.ò*
>
> (Interview ID 644, 26 years, male, Slovakia)

The reference to the large number of victims of the same crime may be interpreted as an attempt to rationalise the ubiquity of such crimes or the potential dangers associated with the Internet and the digital more generally. There are a few other stories of victimsô experiences

that did not relate to data and could not be categorised accordingly. However, many others were different. Respondents who were a victim of crime that happened in public space (e.g. mugging, violent assault) for instance, often made comments about CCTV cameras. However, as they often did not help to prevent the crime, statements were rarely in favour of this technology as a preventive measure. It also seems that preventive measures against burglary, mugging or other more Ăpublicñ crimes are easier to install, such as *martial arts*, *Ăgood running shoesñ*, *Ăa big lockñ* (on the bike or door) than measures against Internet and data related crimes, hence the reactions towards the latter tends to portray more resignation than reactions towards the former. Overall a certain acceptance of these forms of non-violent crimes seems to be prevalent among our interviewees, which may also be interpreted as a form of resilience.

2.6 CONCLUSION

As laid out at the beginning or this chapter, we wanted to explore the dilemma that exists with regards to electronic consumerism and online activity on the one side and issues of data protection on the other. We used interview data gathered in five countries to find common narratives of how this dilemma is addressed, expressed and rationalised within the everyday lives of our respondents. In examining this dilemma through different focal points ï i.e. loyalty cards, online shopping, internet usage and victim experiences of online crime ï we were able to identify a few overarching themes or narratives of how the assumed dilemma was rationalised and coped with in everyday life. These can be seen as prototypical reactions or coping strategies.

- ð *ĂWhat can I do?ñ* This is in essence what many interview partners responded when asked to assess their own engagement with the world of digital consumerism. They were aware of the data protection issues regarding the commercial realm, but were engaging with it anyway, not least because they assumed they had no other choice.
- ð A less fatalistic approach came through in a reaction that can be termed Ătrade-off as a bearable nuisanceñ. The respondents were not happy about the abuse of their data, but accepted it as something they had to go along with, not least because it gave them amenities and provided for the conveniences of many aspects of their daily lives.
- ð A rather more positive version of this previous reaction or assessment of the trade-off, emphasises the bargains, benefits and received goods that can be obtained in exchange for the personal data provided. Respondents speak of exchanges or actual deals.
- ð Being a victim of online or Internet fraud ï also referred to as cybercrime ï is a reoccurring experience within all of these cases, especially the first one of Ăwhat can I doñ. Compared with other security issues, such as personal assault, muggings or burglaries, these kinds of crimes are seen as less intrusive and frightening.
- ð The respondents are well aware that digital consumerism is an integral part of everyday life, which has pitfalls, negative sides, but very often also provides new conveniences for which a certain amount of personal data may be traded. If not willingly then with an indifferent acceptance, or ï rather rarely ï with an effort to resist or better prepare for existing threats. A very important way of coping with these issues is what we refer to as the management of privacy, although this does not necessarily mean that the strategy is

effective. However, it shows that the problems as such are reflected and coping strategies are developed based on this reflection.

- Yet another different way of coping can be found in arguments that stress the fact that ñeverybody does itò, i.e. justifying the action with reference to others who act in the same way.
- And finally we have found various stories that refer to something we call security fatigue. This is often based on a lack of bad experiences concerning the abuse of onesô data. The threat appears to be too abstract to be reckoned with on a daily basis, and indeed it seems tiresome to individuals to constantly pay attention to digital pitfalls.

Throughout the interviews statements on privacy, data, the uses of data in everyday life, the personal encounters with data collection and the respective assessments were often embedded in a narrative of Ămanagingñ data and privacy (thus hinting at a concept of Ădoing privacyñ) in everyday life. This narrative of what could be termed Ăprivacy managementñ or ñprivacy labourò occurs in various contexts and to various degrees throughout many interviews, as do statements referring to data protection and privacy issues. As data and privacy issues become relevant in more mundane, everyday activities, the digital appears to be an inseparable part of everyday life. Accordingly, managing privacy and personal data implies the existence of routines and socio-cultural Ăscriptsñ that are followed to cope with the many requirements and demands of a digital information society in everyday life. The pervasiveness of the Internet in all its forms is apparent and has long become a part of everyday life and practices - socially, culturally and economically. To frame this under the term surveillance may thus be misleading as many of those measures and strategies are not driven by a desire to control the citizen in the sense of an authoritarian state, but to make money ï hence knowing and managing the customer is paramount here. But as much of these strategies appear in the everyday contexts of Europeans, the perceptions of these strategies and the attitudes towards the data collection behind them, may be framed differently than in terms of surveillance and control.

Together these two developments irreversibly have put questions of data protection and online security back on the agenda of citizens, in contrast to previous years. As a result this has massively sharpened the dilemma that we have outlined here.

Final reflections on modes of surveillance: private versus state

This leads to yet another finding of our analysis, namely the focus on different modes of surveillance: private/corporate vs. state surveillance. The boundaries between the two are increasingly blurred: CCTV is situated in public as well as private spaces; it is likely that private companies possess increasingly detailed data than agencies of the state (with the exception of the NSA); and both private and state surveillance increasingly rely on algorithms to gather, process and analyse data.

However, both areas are perceived differently and hence are subject to different discourses and debates: Surveillance is what the state does and it is labelled accordingly. Surveillance is perceived as an Ăassaultñ on the Ădeviantñ citizen, as a threat to the individual and his freedom and rights. It is the person as such that is the aim of these kinds of surveillance Ăattacksñ. The individual is defenceless and naked. The NSA and others are no longer old school spies eavesdropping from the neighbouring room or via miniature bugging devices, but

complex organisations that run high-end computer systems that look for keywords in data collections, constructing new relations based on temporal, social or other indicators. The relatively small protest against new surveillance infrastructures such as INDECT may be interpreted as a general lack of awareness of how these developments may impact on personal lives in general. Instead, as our interviews have shown, the Ăclassicalñ image of state surveillance prevails, an image, which is oriented on the person, aimed to infringe on personal freedoms in order to control and manage the person and his/her good conduct within society. To a much lesser extend this holds true for the perception of the corporation; in this case control and surveillance are framed as a trade-off, a deal or a bearable nuisance.

Within this logic the literary model of George Orwellôs Ă1984ñ is cited time and time again. Orwell portrayed this particular form of surveillance, in which concrete persons (Winston Smith, Julia) are controlled by others (OôBrian) or watched and later threatened, tortured, killed or forced to change behaviour by personalised entities (Big Brother). All of this is linked to a totalitarian state that neither protects people, nor gives them any kind of advantage. The individual is threatened.

Corporate activities by companies such as Google and Amazon, from data collection to customer profiling, do not seem to be perceived in the same way. They are not identified as a mode of surveillance in the Orwellian sense. Responses refer to these activities as Ădata usageñ that are made by anonymous entities, not by persons, but through algorithms. These procedures do not represent an attack on the individuality or the freedom of choice ï the biggest problem identified here lies in the fact that data can be sold, hence it is an attack on private property. However, corporate Ădata usageñ does provide advantages: Discounts, bonus points and special offers are welcome benefits, as long as the gathered data is not sold or otherwise redistributed. This would devalue the trade that has been made by disclosing personal data in return for these advantages.

Interestingly the discussion about private/corporate surveillance does not refer to a particular literary model (although Big Brother is evoked from time to time). Aldous Huxleyôs ĂBrave New Worldñ would provide a very fitting model. However, Huxleyôs work in which the brave new world is less a threat than a seduction through drugs and other offers of happiness, is not chosen as a reference. Rather, our interview partners try to take refuge in silence or suppression ï *ĂI donôt want to think about it, as it would make my life too complicated or impossible...ñ*. The dependency on the digital world ï particularly among young people ï seems to be so all-encompassing, that possible limits to personal freedoms of choice or fears on how their own behaviour is managed by the digital actors, are rendered insignificant.

It is interesting to note that private/corporate surveillance on the one hand and state surveillance on the other are perceived so differently ï despite the fact that they increasingly come to resemble each other in terms of technology. It seems that potential threats are rationalized differently. While state surveillance is a political threat aimed at the person (freedom of speech, freedom of choice, censorship etc.), private/corporate data usage is a problem of personal/private property and its management. The latter is situated within the world of consumption and linked to possible monetary benefits or gains. Against this background we identified different ideas of Ăresilienceñ among our interview partners. In the case of political surveillance, resilience is associated primarily with political protest and resistance (although not necessarily active resistance). With regards to private/corporate surveillance, resilience takes the form of ignorance or indifference.

It is debatable whether such a reading of resilience is sensible or even acceptable. It may well be that the digitisation has also produced a new normality that forces the revision of classical concepts of subjectivity, privacy and freedom of choice.

Indeed, our interview partnersô responses indicate a structural change within the security discourse itself. This discourse, which has previously been characterised by an idea of steady security accumulation, i.e. that the level of security may be raised through particular activities or investments, it now becomes clear that there is no such thing as ñtotalò security. In the discourse on the use of nuclear power for instance this perspective has been introduced with the recognition of "residual risks". Although no one speaks of residual risks in a digital world, we can identify aspects of such a diffuse uncertainty therein. When it is too complicated to implement current security options, and even professional companies are not able to make their own systems secure, it is of no surprise that lay persons develop a "security fatigue". Against this background, 'resilience', (understood here as a form of resistance against multiple threats) seems to be realized neither by the rejection of monitoring practices, nor a continuous enhancement of security (at least when concerning private/corporate surveillance). Instead we can observe a certain indifference and "security fatigue". If one is too concerned with possible threats beyond agreed minimum standards, it seems almost impossible to move freely and carefree in the digital world. In addition to the aspect of resistance, resilience also implies the capability to move or exist in a ñhostileò environment that is not characterized by a continuous progress in security, but rather by permanent uncertainty. Such uncertainty has to be bypassed. Under such conditions surveillance measures of various kinds are either accepted helplessly or reinterpreted as rather unproblematic ñmeasures of data usageò.

3 2ND DILEMMA: PRIVACY AND SECURITY

3.1 INTRODUCTION: SECURITY TECHNOLOGY AND TECHNOLOGICAL SECURITY

Reinhard Kreissl

Security at the level of citizens is primarily discussed as perceived security. Over the last decades the concept of perceived security or subjective security has attracted attention in academic and policy discourse. There are a number of reasons for this replacement of security with perceived security. First of all the figures of registered crime, crime being the dominant source of insecurity for a long time, are not representative of the development of criminal behaviour. They primarily reflect activities of law enforcement agencies, i.e. more police creates more (registered) crime, more reports of incidents by citizens to the police lead to higher crime figures. Secondly, as criminological research on victimization and fear of crime has demonstrated, levels of perceived insecurity do not mirror objective victimisation risk: persons with statistically low probability of victimization often display high levels of fear or insecurity and vice versa. As fear of crime studies have repeatedly demonstrated, levels of fear of crime reflect other, broader existential insecurities.[84] Law enforcement agencies thus have begun to focus on feelings of insecurity as public sentiment, while at the time acknowledging the limitations of combatting or reducing crime in the literal sense.

Security technology in the broadest understanding of the term introduces a new element in the ecology and dynamics of (in)-security. Under conditions of relatively high levels of perceived insecurity, technology can help to ease these feelings. Asking citizens which measures they would prefer to increase security, many surveys produce similar results: technological security measures and increasing surveillance both score high on the list of preferred measures. Installing CCTV in public places is perceived as an effective security measure. Increasing checks, controls, and scanners at airport gates is also seen as having a positive effect on security. But at the same time, the manifold forms of flagging insecurity by introducing visible security technology can foster a feeling of insecurity. So the evidence is mixed. It is hard to determine whether security technology has an overall positive effect on perceived (in)-security of citizens. This is due to the paradoxical nature of feelings of security. Security as a subjective mental state is predominantly a by-product, i.e. a person feels secure, when s/he is not reflecting on his/her security. As soon as s/he starts to think consciously about how secure s/he feels in a given situation a cognitive frame is activated, scanning his/her environment and inner state along the dimension of security/insecurity. This paradoxical constellation is similar to the well-known communication paradoxes, e.g. when a person is addressed with a message like: ñBe spontaneous!ò Being or acting spontaneously cannot be achieved by will or as a reaction to a request. The same holds for security.
While on the one hand the desire for more and better security technology is fuelled by feelings of insecurity or growing fears of security threats, every new technological add-on creates new insecurities. This is a dynamic of addiction: increasing security measures fosters

[84] Comp.e.g. Ditton, Jason and Stephen Farrall, *The Fear of Crime*, Ashgate/Dartmouth,2000.
Lewis, Dan and Greta W. Salem, *Fear of Crime: Incivility and the Production of a Social Problem*. New Brunswick: Transaction Publishers, 1986.
Vanderveen, Gabry, *Interpreting Fear, Crime, Risk, and Unsafety: Conceptualisation and Measurement*. Boom Juridische Uitgevers 2006.

insecurity which then in turn triggers the demand for more security measures. Breaking this vicious cycle of security technology and technological security is difficult ï like with all addictive behaviour.

What supports the demand for security technology is an approach that outspoken critics like Morozov have termed ñtechnological solutionismò or ñtechno-fixò[85]. This approach takes on different forms. One version is based on the assumption that security problems can be successfully addressed, when they are identified at an early stage. The best way to identify such emerging problems is to keep the environment under constant surveillance in order to detect warning signs or potential predators before any damage materializes. Another variety of solutionism operates with the idea of target hardening: A potential object of an attack is equipped with technological fences and locks, controlling the access. The prototype for this variety would be the gated community, as a space, where residents take all measures to keep potential security threats (spelt out as non-resident criminals) out.

The different varieties of technological solutionism also create an added value in a political context. Security issues can be translated into problems of accountability. Whenever a security problem is identified and accepted as such the question emerges, who has to take remedial action to prevent future damage and what kind of action would be appropriate for the given problem. To address a publicly accepted security problem a responsible political actor has to take appropriate measures to react to the emerging threats. Since many issues on the political agenda can be redefined as security problems, a process, which has been defined as ñsecuritizationò, policy actors feel the need to react. One of the most convenient options in such a situation is the implementation of surveillance and security technology. Working within the mind-set of solutionism, technology always entails the promise of remedy. From a political perspective it is the promise that counts. Whether a new technology or surveillance measure will live up to the promises of the suppliersô marketing brochures is often hard to determine.

With security as one of the political and cultural main frames, individual citizens are also addressed to take precautions in their daily lives and environment. Being a prudent citizen is perceived as a key challenge in present day societies. Taking precautions, constantly screening the world for risks in order to prevent future damages is part and parcel of laypersonsô reasoning. This preventative turn in many fields of everyday life[86] (from health to crime) is reinforced by a number of governance strategies implemented by public authorities and private enterprises alike. The premium for health insurance may be lower for those individuals, who can demonstrate a healthy life style and regularly take health checks. Police can advise citizens to be on the alert, communicating local threat assessments to the public (ñBeware of burglars!ò). Technology is an important element in this context as well. Installing private video cameras or burglar alarms on oneôs premises is perceived as a meaningful way to protect life and limb. Monitoring the performance of your physiological system is perceived as a form for self-enhancing biofeedback. Again technology here holds a promise to

[85] Morozov, Evgeny, *To save everything, click here. The folly of technological solutionism*, Public Affairs, New York, 2013.
[86] Luhmann, Niklas, Risiko und Gefahr, In. *Soziologische Aufklärung, 5*, 2 Auflage, Opladen, Westdeutscher Verlag, 1993, pp. 131 -169.

increase security (or hardening the target of oneôs body). It is understood as a tool, helping to keep the forces of evil out through early detection, deterrence or prevention.

This understanding of technology as a tool to be used like a wrench or a screwdriver ignores the pervasive nature of technology-use, the effects technology has on human lives and the incorporation of cultural and social structures in the materiality of technologies.[87] It creates many futile controversies about (benevolent) use and (malevolent) misuse of technologies ignoring the ñautonomyò of all technology.
Such issues are addressed in Science and Technology Studies (STS) or Actor Network Theory (ANT), although both of these approaches do not address security problems as their main topics of interest. But the conceptual ideas from both of these approaches can be applied to the analysis of security as an element of citizensôeveryday life.

Technology makes objects visible (letôs them appear), enables remote and onsite social sorting, extends the range of perception and communication, injects the idea of objective knowledge in the debates about security, threats and vulnerabilities. While in surveillance and critical legal security studies, technology is seen as a means to widen and deepen the panoptic gaze or as a force to be tamed by proper constraining legal measures, a number of questions are ignored with regard to the role of security technology and the working of technological security. The autonomy of technological systems can be studied nicely in areas like high frequency algorithmic trading in the financial system or in the effects of automatic web-tools, creating more traffic on the Internet than human users do.[88] Technology simply by its use changes the world in many different ways. And it also changes the life-world of the ordinary citizen in a myriad of ways, some of them related to security, surveillance and fear.

Investigating these effects with a focus on security and surveillance is the key objective of this chapter. While from the surveillance studies expertsô perspective, the massive surveillance potential of technological systems is the dominant focus, there are other ñeffectsò of technology that have to be considered. Surveillance technologies permeating everyday life can have subtle and remote effects beyond the intended societal domains. Making these effects visible is one of the main objectives of this chapter.

3.2 CCTV IN EUROPE

Chiara Fonio

In the last few decades, the diffusion of CCTV both in public and private spaces in Europe has grown gradually but systematically. Despite this proliferation, the use and the regulation of surveillance cameras vary widely across the continent; one might argue that CCTV is now a routine feature of security in modern European cities. Notwithstanding significant national differences, if compared with other surveillance techniques like dataveillance, CCTV is one of the ñoldestò and most studied security tools within the cross-disciplinary field of

[87] Woolgar, Steve, and Neyland, Daniel, *Mundane Governance. Ontology and Accountability*. Oxford Univ. Press, Oxford, 2014.
[88] Madrigal. Alexis, http://www.theatlantic.com/technology/archive/2013/12/welcome-to-the-internet-of-thingies-615-of-web-traffic-is-not-human/282309/

ñsurveillance studiesò[89]. CCTV epitomizes the archetype of contemporary surveillance[90] and not only is the literature rich, but it has drawn attention to a myriad of complex socio-economic and cultural dimensions which seem to constitute the framework of the far-reaching rise of CCTV cameras. As Norris puts it, ñwhen we are trying to understand the rise of CCTV as a global phenomenon we should not only see it as a technology but a discursive object. A discursive object waiting to be deployed in public debate as a response to the latest perceived crisis [é]ò[91].

The development and the use of CCTV in Europe from a comparative perspective, has been documented by empirical studies such as the UrbanEye Project[92]. This research was carried out from 2001 to 2004 involving seven countries: Austria, Denmark, Germany, the United Kingdom, Hungary, Norway and Spain. As an in-depth analysis of the UrbanEye data goes beyond the aim of this short introduction, it will suffice to look at common trends and differences[93]. The data suggest that there is a significant difference between the diffusion of surveillance cameras in the United Kingdom and other countries involved in the project. The diffusion or the technological sophistication in public and semi-public spaces is most advanced in the UK (40%) and least developed in Austria[94]. The numbers demonstrate the wide variety between countries: ñwhile it was estimated that around 40,000 cameras monitor public areas in more than 500 cities in Britain, less than 100 cameras monitor public areas in around 15 German cities, and no open street CCTV system is in operation in Denmarkò[95]. When asked for their attitudes towards CCTV, the majority of respondents in all five capital cities (in Austria, Germany, the UK, Hungary and Norway) seemed supportive of surveillance cameras ñwith Britons being most supportive and Austrian and Germans being rather scepticalò[96]. The data also show that the locations of cameras play a relevant role in terms of acceptance: while CCTV at banks or at subway platforms is not questioned, the use of cameras in changing and/or fittings rooms in sport centres and shops is considered much more problematic[97]. It is also worth noting that two thirds of respondents agreed with the statement ñnothing to hide, nothing to fearò but more than half thought that the footage could easily be misused[98].

The UrbanEye project remains the only comparative European study focused on surveillance cameras. However, there is a considerable amount of literature, which documents camera

[89] Lyon, D., *Surveillance Studies: An Overview,* Polity Press, Cambridge, 1997.
[90] Doyle, Aaron, Randy Lippert and David Lyon (eds.), *Eyes Everywhere. The Global Growth of Camera Surveillance,* Routledge, New York, 2012.
[91] Norris, Clive, ñThereôs no Success like Failure and Failureôs no Success at all: Some critical reflections on understanding the global growth of CCTV surveillanceò in Doyle, Aaron, Randy Lippert and David Lyon (eds.), *Eyes Everywhere. The Global Growth of Camera Surveillance,* Routledge, New York, 2012, p.40.
[92] www.urbaneye.net
[93] For an overall analysis of the final findings see: Hempel, Leon, and Eric Toepfer, *CCTV in Europe. Final report,* Working Paper No.15, Centre for Technology and Society, 2004, http://www.urbaneye.net/results/ue_wp15.pdf
[94] Hempel, Leon, and Eric Toepfer, *CCTV in Europe. Final report,* Working Paper No.15, Centre for Technology and Society, 2004, p.5 http://www.urbaneye.net/results/ue_wp15.pdf
[95] *ibidem.* It is worth noticing that the situation in the above-mentioned countries is probably quantitatively and qualitatively different from the picture that emerged in the UrbanEye project. For instance, in 2012 in Denmark 2,200 cameras were mapped http://www.journalism.co.uk/news/data-journalism-crowdmapping-denmark-s-cctv-cameras/s2/a550761/ Accessed on 01/07/2014.
[96] Hempel, Leon, and Eric Toepfer, *CCTV in Europe. Final report,* Working Paper No.15, Centre for Technology and Society, 2004, p.42 http://www.urbaneye.net/results/ue_wp15.pdf
[97] *ibi*: pp. 43-44-45
[98] *ibi*: p. 45

growth, CCTV regulation and the potential impact of cameras[99]. More often than not, there is a distinction in the literature between the development of CCTV in the UK and elsewhere. In contrast to the rest of Europe, in the UK substantial government investment in crime reduction schemes have promoted an unparalleled diffusion in the public space. Norris argues that ñit is not unreasonable to estimate that between 1995 and 2005 over £500 million of central and local government funds was allocated to CCTVò[100]. This has also led to a proliferation of studies within the British national context which have revolved around lines of, *inter alia*, asymmetries of power between the watchers and watched[101], the evaluation and the regulation of CCTV[102], the rationale behind the policy of CCTV cameras[103], etc.

Despite the growth of surveillance cameras in other European countries being more ñsilentò[104], CCTV is now ubiquitous, especially in urban contexts. The emergent picture is an increasing ñnormalizationò of (video) surveillance technologies, meaning not only an increasing number of cameras but also ñhow these are embedded in the norms and institutions of society and how they are reflective of other aspects of modern societyò[105]. Living under the gaze of CCTV is, especially after Islamic terrorism hit European soil, normal even in countries where the shadows of an authoritarian past are still present[106].

For the purpose of this chapter, we will limit the discussion to the countries involved in this part of the IRISS project, namely Austria, Germany, Slovakia, Italy and the UK.

The UrbanEye report on Austria[107] has drawn attention to the use of video surveillance in traffic management, public transport and to specific areas of the capital where CCTV is in place to protect government buildings. It seems that, due to low crime rates, the number of open-street cameras or the public debates are limited. In 2014 only 18 ñhot spotsò, defined as areas with high crimes rates, are monitored by the police through CCTV. One would not find

[99] *Inter alia*, the special issues published in *Surveillance & Society:* ñThe Politics of CCTV in Europe and Beyondò Vol. 2, No 2/3 2004: http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/CCTV; ñRevisiting Video Surveillanceò Vol 6, No 1 (2009): http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Relaunch. And more recently the issues published in *Information Polity*: ñRevisiting the surveillance camera revolution: issues of governance and public policyò Vol. 16, no 4 2011: http://iospress.metapress.com/content/h03500355222 ; ñRevisiting the surveillance camera revolution: issues of governance and public policyò, Vol. 17, No 1, 2012: http://iospress.metapress.com/content/r161232517m7

[100] Norris, Clive, ñThereôs no Success like Failure and Failureôs no Success at all: Some critical reflections on understanding the global growth of CCTV surveillanceò in Doyle, Aaron, Randy Lippert and David Lyon (eds.), *Eyes Everywhere. The Global Growth of Camera Surveillance*, Routledge, New York, 2012, pp. 23-45.

[101] Most notably, the seminal work of Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999 and MacCahill, Michael, *The Surveillance Web: the rise of Visual Surveillance in an English City*, Willan, Collumpton, 2002.

[102] *Inter alia*: Webster, W., ñThe Diffusion, Regulation and Governance of Closed-Circuit Television in the UKò, *Surveillance & Society*, Vol.2 (2/3), pp. pp. 230-250. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3376/3339

[103] *Inter alia*: Webster, W., ñCCTV Policy in the UK: Reconsidering the Evidence Baseò *Surveillance & Society*, Vol. 6, No 1(2009) pp. 10-22 http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3400/3363

[104] Fonio, C., ñThe silent growth of video surveillance in Italyò, *Information Polity*, Vol. 16, No 2/2011 pp. 379-388: http://iospress.metapress.com/content/d187624350281110/

[105] Murakami Wood, David and William Webster, ñLiving in Surveillance Societies: the Normalisation of Surveillance in Europe and the Threat of Britainôs Exampleò, J*ournal of Contemporary European Research*, Vol.5, No 2 (2009) pp. 259-273 http://www.jcer.net/index.php/jcer/article/view/159/144

[106] See, for instance, the implementation of video surveillance in Portugal: Frois, Catarina., *Peripheral Vision. Politics, Technology and Surveillance*, Berghahn Book, Oxford, 2013.

[107] Ney, Steven and Kurt Pichler, *Video surveillance in Austria*, Working Paper No. 7, Interdisciplinary Centre for Comparative Research in the Social Sciences, 2002, http://www.urbaneye.net/results/ue_wp7.pdf

larger parts of cities under CCTV surveillance, as is common in British cities. Of course public private spheres such as shopping malls are monitored more frequently but a CCTV camera in public space remains rather uncommon phenomena According to a survey conducted in 1999, 84% of Austrian citizens are in favour of video surveillance only if it is used to fight violent and serious crime. Additionally, more than half do not think that ñnew tracing methodsò are invasive of their privacy. However, while Googleôs Street View is not CCTV as such, the fact that it was banned in Austria is indicative of a certain level of public awareness as far as surveillance and privacy are concerned.

In Germany the use of CCTV in public spaces is neither ñnewò[108] nor overlooked in the public debate[109]. The UrbanEye project documented the ñinescapabilityò from the gaze of surveillance cameras in the city of Berlin. However, in contrast to other European countries, in Germany the freedom to reveal *or hide* personal data made the use of CCTV highly controversial[110]. In 2013 many cameras were trashed in Berlin ñto protest against the rise in close-circuit television across Germanyò[111] Despite differences in purpose and sophistication, surveillance cameras have rapidly expanded in Germany. Toepfer argues that since 2004, Germany has doubled the number of cities where CCTV is operating, from 15 to 30[112].

In Italy, the literature on video surveillance is very limited. While there are no assessments at a national level pertaining to the effectiveness of CCTV in preventing crime and/or public attitudes towards surveillance cameras, emerging trends are not dissimilar to the rest of Europe. The increasing number of cameras in Italian cities did not go unnoticed and the DPA issued the first ñguidelinesò in 2000 due to the steady growth of video surveillance both in public and private spaces. Moreover, the only qualitative research[113], carried out in the city of Milan, confirms findings that also emerged elsewhere[114], namely categorical suspicion and the exclusionary features of this tool. However, due to the lack of empirical data it is difficult to infer overall tendencies. Yet, it is worth mentioning that the decentralization of security policies has impacted on the implementation of CCTV at a national level.

Data on the use of surveillance cameras in Slovakia are almost non-existent, except for concerns raised by Privacy International, which highlighted that, in 2007 and 2008, many CCTV systems in Bratislava and in other municipalities were in breach of privacy[115]. There is no public debate and the media seem to report on new implementations of surveillance

[108] Kammerer, D., ñPolice use of public video surveillance in Germany from 1956: management of traffic, repression of flows, persuasion of offendersò, *Surveillance & Society*, Vol.6 No.1, 2009, pp. 43-47, http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3403/3366

[109] See, for instance: http://www.dw.de/germany-debates-surveillance-cameras-after-boston/a-16760452

[110] Hempel, Leon and Eric Toepfer, *CCTV in Europe. Final report*, Working Paper No.15, Centre for Technology and Society, 2004, p.62 http://www.urbaneye.net/results/ue_wp15.pdf

[111] Stallwood, O., ñGame to destroy CCTV cameras: vandalism or valid protest?ò , *The Guardian*, 25/01/2013 http://www.theguardian.com/theguardian/shortcuts/2013/jan/25/game-destroy-cctv-cameras-berlin Accessed on 22/04/14.

[112] In Norris, C., *A review of the increased use of CCTV and video-surveillance for crime prevention purposes in Europeò* Civil Liberties, Justice and Home Affairs, April 2009, p.10 http://www.statewatch.org/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf

[113] Fonio, C., ñThe silent growth of video surveillance in Italyò, *Information Polity*,Vol 16, No 2/2011 pp. 379-388: http://iospress.metapress.com/content/d187624350281110/

[114] *Inter alia*: Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999; Mork Lommel, Heidi., ñTargeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norwayò *Surveillance & Society*, vol. 2 (2/3), 2004 pp. 346-360 http://www.surveillance-and-society.org/articles2(2)/unwanted.pdf

[115] https://www.privacyinternational.org/reports/slovakia/ii-surveillance-policies#footnote18_8o5n4kx. Accessed on 22/05/2014.

technologies (it is estimated that that in the old centre of Bratislava there are 187 publicly and privately-owned surveillance cameras[116]) without disputing the actual need for them[117].

As mentioned above, there is a significant amount of research and a number of theories, which have attempted to explain CCTV intensification in the United Kingdom. In the late 90s, 86% of local authorities had installed CCTV systems in public places and, as argued by Webster, ñ*CCTV had become a core element of law and order policy, for both government and opposition parties, and politicians have been keen to promote the virtues of technologies***ò**[118]. In 2013, the British Security Industry Authority estimated that there are up to 5.9 million CCTV cameras in England, 750,000 of which are in ñsensitiveò locations like schools, hospitals and care homes[119]. In particular, a report released by Big Brother Watch in 2012, drew attention to the sheer amount of CCTV used in secondary schools and academies in the United Kingdom where the total number of cameras used by 2,107 schools is 47,806[120]. A comprehensive summary of what has emerged from the rich scholarly literature on the UK cannot be given here, however, drawing on Norris[121], there are a few aspects which are worth considering: a) evaluations on the effectiveness of CCTV have been contradictory; b) a British Home Office evaluation in 2005 reported that CCTV does not reduce fear of crime; c) the use of CCTV footage in investigations is far from certain and d) CCTV could have social implications (i.e. the exclusion of already marginalized minorities).

Having this complex framework in mind, we now turn to analysing narratives around CCTV, drawing on quotes from the interviews. The analysis is articulated around topics and hypotheses, which arose from the interviews.

3.2.1 General opinions on CCTV

As stated in the introduction, the use of surveillance cameras is nothing new in Europe. One might argue that European citizens are familiar with CCTV and that the use of surveillance cameras is now taken for granted. Not only are citizens familiar with this surveillance tool but, as documented by the research analysed in previous pages, large parts of society are supportive of CCTV. Living under the gaze of the cameras, in cities and in small municipalities alike, can be considered as an embedded feature of todayôs surveillance societies. Therefore, we expected to deal more with the ñnothing to hide, nothing to fearò argument than with people who seem to question the normalization or the effectiveness of the cameras. The standard explanation given by citizens for thinking positively about CCTV in various contexts was, that they had nothing to hide and therefore nothing to fear. Asked about

[116] Source: Accessed on 22/04/2014.
[117] Durinanova, M., ñ*Cameras cut down on Bratislava city crime*ò, The Slovak Spectator, http://spectator.sme.sk/articles/view/22527/3/ Accessed on 22/05/14.
[118] Webster, W., ñ The Diffusion, Regulation and Governance of Closed-Circuit Television in the UKò, *Surveillance & Society*, Vol.2 (2/3), p.237 http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3376/3339
[119] Barret, D., ñ*One surveillance camera for every 11 people in Britain, says CCTV survey*ò, 10/07/13,The Telegraph, http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html Accessed on 01/07/14
[120] A Big Brother Watch report, *Class of 1984. The extent of CCTV in secondary schools and academy*, 2012, http://www.bigbrotherwatch.org.uk/files/school_cctv.pdf
[121] Norris, Clive, ñThereôs no Success like Failure and Failureôs no Success at all: Some critical reflections on understanding the global growth of CCTV surveillanceò in Doyle, Aaron, Randy Lippert and David Lyon (eds.), *Eyes Everywhere. The Global Growth of Camera Surveillance*, Routledge, New York, 2012, pp. 23-45.

the CCTV cameras at the local airport for example, many citizens explained to us that if CCTV helps to prevent future terrorist attacks it is a good tool for law enforcement in their views. Depending on the location of CCTV a general attitude that could be found in the material was that CCTV is a profound measure to prevent crime. In other words, we expected that the proliferation of CCTV has to some extent and with significant national variations, ñsettledò both in the psychological and in the urban landscape. However, this is certainly not true for all respondents and stories collected for this report. While CCTV is ubiquitous, issues of proportionality, effectiveness, regulation and privacy were raised by a number of interviewees. The steady proliferation of surveillance cameras does not make them more acceptable. Additionally, concerns on the overall approach to security seem to be significant to the respondents.
The following quote, for instance, epitomizes criticism towards the use of CCTV for security purposes:

> ñ*Well how should I put it? Itôs the wrong way to solve a real problem. That there is vandalism and that people get robbed, those problems exist. But you canôt solve them with video surveillance. At BEST you can solve the crime and not even this works every time and it also delivers a wrong feeling of safety that there is someone who is watching. This leads to people not being cautious themselves anymoreò*
>
> (Interview ID 794, 36 years, male, Austria)

When prompted about his general views on video surveillance, this respondent answers that CCTV is not effective in dealing with ñrealò security problems. Moreover, he emphasizes the risks of delegating personal safety to someone else. This points also to the role of technology, which, instead of being a socio-technical tool used for security reasons, has gradually *colonised* the social to the point that people are not ñcautiousò anymore. He does not deny the fact that there are security problems but instead he seems to question the way in which problems are dealt with. It becomes clear that the narrative revolves around issues of effectiveness and also of false feelings of security. Even though the interviewee does not develop his argument further, his opinions are straightforward: relying on CCTV does not always work and it also conveys distorted sensations. This quote shows that the overall approach to either security or safety, embodied by cameras, is criticised.

Other respondents also addressed issues of asymmetries of power along with general concerns for the normalization of surveillance among the general public:

> ***ñ****I accept the use of CCTV systems per se, but I do not trust the way the footage is managed and what it is used for: whoôs watching whom? People are getting used to video surveillance, when it was something new, people immediately criticized this technological tool and they were confused by CCTV, but now nobody bothers about CCTV anymore and they do not look at the video-cameras anymore. This is a system that functions for those who have the power, as a control instrument, which, although at the beginning it was not accepted, because nobody removed CCTV systems, everybody passively got used to it and the citizen has no power to contrast this situationò*
>
> (Interview ID 574, 48 years, male, Italy)

In this case, the interviewee is not against the surveillance tool as such but nonetheless expresses his concerns in relation to: a) the ways in which CCTV is used, b) the passive acceptance of CCTV by citizens, c) the issue of power, and d) the impossibility to resist the increasing use of video surveillance. Moreover, the respondent frames the argument along lines of trust by questioning who the watchers and the watched are and why CCTV is used. This account is of particular interest as it points to several dimensions; one of them being criticism against the alleged normalization of CCTV. In his view there has been a shift: from criticism of video surveillance to acceptance. This citizen seems concerned about the normalization of video surveillance without being ñagainstò it. It is worth noting that surveillance cameras are directly related to issues of control and power. If, on the one hand, the watchers have power over the watched, on the other the watched ï being increasingly accustomed to the use of surveillance ï are now disempowered. To him, disempowerment goes hand in hand with acceptance. Resistance is not even an option or, at least, it is not an option anymore. Additionally, the issue of trust between citizens and the watchers is raised.

There are several statements on CCTV footage. Interestingly enough, questions on video surveillance footage were not asked directly but, as we also examine in paragraph 5.2.3, this is obviously an important topic to the citizens we interviewed. In fact, this issue was addressed by interviewees answering general questions on cameras.

> ***ñ****In general, I can agree with the use of CCTV cameras if the data show that it helps bring down crime. I think that the request for the use of these devices from the law enforcement side is relevant. However, I**ô**m not sure about the way the use of records is regulated. I can see some possible negative consequences, breach of human rights. So I can see some potential danger, because we have recently seen what was going on in the USA with surveillance. So it has to be strictly regulated**ò***
>
> (Interview ID 739, 26 years, male, Slovakia)

This respondent is not opposed to the use of CCTV but he argues that the effectiveness of the tool has to be corroborated by figures on crime rates and that it has to be rigorously regulated. In particular, the regulation of CCTV pertaining to the use of footage is considered as a safeguard against potential misuses. He also stresses that the demand for more CCTV comes from police forces and that, in light of recent global surveillance disclosures, the dangers of surveillance have to be taken into account. Once again, like many others, this respondent does not blindly support the use of cameras but rather articulates a discourse in which effectiveness, regulation and the social impact of CCTV are considered.

The majority of the respondents focusing on general ideas about CCTV are far from being generic. Although descriptive accounts are rare, one might argue that the layperson is not naïve: the mere fact that cameras are widely used does not make them acceptable. Hence, a routine feature of everyday life is ï more often than not ï assessed in terms of effectiveness and regulation.

In order to grasp how people deal with the gaze of the cameras, we now shift from general opinions to real-life experiences as far as the ñwatchersò are concerned.

3.2.2 The watchers and the watched: dealing with CCTV and the feeling of being watched

Discourses on the feeling of being watched, namely the *subjective* dimension ï as opposed to the *objective* dimension which pertains to more abstract ideas on CCTV from a security perspective (see paragraph 3.2.3) ï shed light on if, and to what extent, CCTV affects behaviour. This is of particular relevance as research on this topic is almost non-existent. Some guiding questions constitute the analytical framework of this section. Specifically, we look at the strategies used ï if any ï to deal with CCTV: do citizens try to avoid the gaze of cameras or do they accept it? What do they think the watchers are looking at? The underlying assumption is that if CCTV is not just taken for granted but instead, as described in paragraph 3.2.1, it is often questioned, it might also be that people are uncomfortable if they are constantly being ñwatched overò.

The following quote typifies the complexity of feelings of the ñwatchedò:

> *ñI think when it is at the places where there is a need for it, itôs OK, in banks, or shops. My parentsô house was burgled a while ago and my parents are seriously considering some CCTV, so far we have only a fake camera with a red light, I guess better than nothing. In shops, I had an experience recently, I found a nice pair of trousers, but it was the last pair and I needed to get cash from the ATM, so I tried to hide them behind other clothes. I was very scared about CCTV and looked all around if somebody is watching me. Also, in Tesco, when I try to test a new antiperspirant and there is a sign that says it is forbidden, I try to avoid cameras and try it nevertheless. But it is more about customer service in Slovakia, if I try on a new pair of shoes, they are usually tied together, so once again, in order to try them properly, I have to untie the knot that holds them together, all that while being conscious about CCTV*ò
>
> (Interview ID 622, 23 years, female, Slovakia)

In this case, the interviewee shows both acceptance towards CCTV and uneasiness of being watched in semi-public spaces while shopping. Despite the fact that, in her view, shops are places where surveillance cameras should be used, the impact on behaviour is clearly stated. The terminology used in this context seems noteworthy, as this woman is ñscaredò of CCTV and deliberately tries ñto avoidò the gaze of the cameras. Therefore, the experience of consciously being watched by CCTV renders shopping potentially stressful. Strategies to cope with CCTV range from checking to see if there is CCTV before doing something, to avoiding video surveillance. Being aware of CCTV does not prevent this person from shopping, but rather triggers what can be interpreted as a resilience strategy, namely coping with surveillance through avoidance. This account suggests that acceptance does not imply a lack of awareness and/or insignificant impact either on feelings or on behavioural patterns. While it is true that visibility in the form of surveillance is an unavoidable aspect of todayôs social world, it also holds true that people do not simply comply with the fact of constantly being visible, not even when surveillance is considered legitimate. When people cannot ñnegotiateò visibility dialectically, they seek to evade it. For a number of our respondents, being under surveillance means being ñbotheredò by the sheer fact of being watched, ñspied

uponò or ñstalkedò and questions on whom the watchers are, are raised. Some respondents query who ï and for what purposes ï is watching and argue that they are not at ease with CCTV. Others significantly change their behaviour as they avoid streets with cameras or are much more cautious about things that they do in front of cameras.

> ñ*Lately I went to an area where there are many surveillance cameras. I was bothered by the cameras, I felt spied on but I didnôt know by whom. I was with other people and we were all annoyed by CCTV. When I feel bothered by the cameras in the public space I tend to go where there are no cameras*ò
>
> (Interview ID 41, 27 years, female, Italy)

Once again, the terminology is a key element. Not only does CCTV annoy the respondent, but she feels that someone is watching her and is sceptical about this fact. Not knowing the identity of the watcher causes tensions and the only way to reduce it is going to a space free from surveillance. Thus, resilience options here relate to avoiding surveillance altogether. As opposed to private or semi-public spaces where avoiding entails ñhidingò from the gaze, in the public realm citizens have more opportunities as they look for less-controlled environments.

However, the picture is too complex to be put in terms of acceptance/compliance *versus* non-acceptance/resilience or resistance. The following quote highlights further aspects.

> ñ*Itôs all over the place, isnôt it? Yes, itôs everywhere. é I certainly know that there are some in the [shopping] centre, because I go through there all the time, and I know there is CCTV in there. I imagine itôs all over the city centre, and at road junctions, road corners. It may not be very obtrusive, but itôs there, and itôs in buses. é Iôm trying to think. I try and ignore them, actually, and walk along with my head down, but I think there are certainly some near John Lewis*ò
>
> (Interview ID 888, 70 years, female, UK)

This account is not as ñstrongò as the first two as this woman is not scared of CCTV. Video surveillance is not intruding and yet, while trying to disregard CCTV, she does not want to raise attention and walks with her head down. The level of awareness is high, as the interviewee knows where CCTV is located. This shows a more subtle impact of surveillance, which may be related to the culture of suspicion generated by the very presence of the cameras. The discourse articulates the inevitability of surveillance (not obtrusive but itôs everywhere) and the impact on the act of walking. The respondent is not against the use of surveillance cameras but the constant ñregimes of visibilityò[122] bear consequences on everyday life. Other responses refer to ñbehaving normallyò under the gaze of cameras. The disciplinary power of CCTV, thus, seems to produce ñdocile bodiesò[123] and ultimately leads to conformity. People try to behave ñnormallyò or ñnot suspiciouslyò and this too, we would suggest, is an important aspect of dealing with CCTV from the watched perspective.

[122] Brigenti, Andrea Mubi., *Visibility in Social Theory and Social Research,* Palgrave Macmillan, 2010.
[123] Foucault, Michel., *Discipline and Punish: The birth of the Prison,* Allen Lane, London, 1977.

At the opposite ends of the spectrum, there are also a few respondents who do not mind the cameras and do not feel restricted in their movements or in their actions, but the ñnothing to hide, nothing to fearò argument is rarely formulated. These narratives convey a sense of ñsurrenderò to the situation, especially in the public realm but they relate also to security. The ñnothing to hide, nothing to fearò argument emerges when CCTV is linked to security and/or to the inevitability of surveillance cameras in order to deter crime in public and semi-public spaces. Positive attitudes towards CCTV often reveal trust in technology and in law-enforcement. Nevertheless, as mentioned above, optimistic views or lack of concerns for privacy are seldom, when compared to more cautious opinions.

3.2.3 CCTV and crime prevention

In this chapter we analyse what might be called the *objective* dimension of video surveillance. In particular, we look at narratives on CCTV from a security perspective, which deals more with thoughts on the effectiveness of this tool rather than with potential implications on behaviour. There appear to be differences between normative statements on surveillance cameras and crime prevention and more descriptive accounts. When it comes to thinking about the cameras at an abstract level, the dilemma of security *versus* privacy is not of particular significance. If CCTV is used for security reasons, it is accepted. Nevertheless, concerns on how footage is used are sometimes raised along with doubts on the usefulness of surveillance cameras as tools for crime prevention. Overall, more ambiguities and contradictory statements than straightforward opinions emerge. The following response, for instance, highlights controversial thoughts on the effectiveness of CCTV:

> *ñNo, I donôt think it prevents crime, but I think it has obviously had a role in tracing criminals. If you see how many crimes have been solved, lately, with abductions, or whatever else, CCTV has had a crucial role.é There is also so much if you, for example, if they are trying to solve a crime using CCTV, more often than not the footage is completely useless, because the cameras have not been looked after properly, or are not functioning, or whatever else, so, yes, I think it's noté usually not intentionally to record more than they're supposed to.*ò
>
> (Interview ID 10, 38 years, male, UK)

This respondent thinks that cameras do not function as a deterrent but rather that they can assist law enforcement after a crime has occurred. It is worth noting that his views on CCTV vary from the tool being central to criminal investigations to the uselessness of the footage in the majority of cases. Yet, privacy concerns are not even mentioned and excessive recording is not considered problematic. Framing a discourse along the lines of security is clearly different from contemplating potential drawbacks of being watched. The trade-off between security and privacy is not often taken into account when respondents are prompted about crime prevention. If privacy is not at stake, the uselessness of CCTV is often mentioned, especially in descriptive accounts such as the following:

> *ñThe mansions here in this area all have CCTV installed but they are only allowed to film as far as the plot boundary. Three years ago we had a case of arson. A series of arson attacks to be correct. Also here, at the bus station, in front of our house. At the*

> *ladyôs house on the other side of the street they burned her letterbox. She had CCTV running on her property and she recorded everything but in court she was not allowed to use the footage, as you are only allowed to film within the boundaries of your property. So she was only allowed to show the shoes of the arsonist. They would have busted him if she was allowed to use her footage from the CCTV camera.ò*
>
> (Interview ID 360, 69 years, female, Austria)

The interviewee describes the use of CCTV in private spaces. While a neighbour has video surveillance, which recorded a pyromaniac, legal restrictions on the use of footage, precluded the opportunity to catch the arsonist. This narrative seems to question the benefits of having surveillance cameras to protect private properties if the footage cannot be used in court. The distinction between public and private space is only relevant in terms of what can be brought to court. Interestingly enough, when the layperson is not the watched but the watcher who uses surveillance tools like CCTV to defend his/her space, the ñregime of visibilityò is fully supported.

In several statements, the overall security approach behind the use of cameras is disputed. Video surveillance can only be effective if there is real-time monitoring or if it is used to support, not to substitute, law enforcement agencies. Crime prevention is seen as a multi-faceted problem that should be addressed with the help of security technologies but there must be a good reason (i.e. high crime rates) to rely on CCTV. Electronic eyes should not be everywhere simply because this is a common trend, rather the training of CCTV operators as well as risks of potential misuses of footage occasionally pop up in the interviews. Some respondents do not understand why surveillance cameras have been implemented and would like to reclaim ñpublic common spacesò:

> *ñI know where the cameras are here and I donôt understand why CCTV was installed. CCTV does not make sense to me because it is only used to watch what has already happened. They are not effective in preventing criminality, theyôre just a waste of money. I can understand the use of video surveillance in private spaces, like in a bank where CCTV can be effective in order to catch robbers. But public squares are ñcommon goodsò, they belong to the citizens. I am really annoyed by the use of surveillance in the public realm.ò*
>
> (Interview ID 91, 52 years, female, Italy)

This respondent struggles to grasp both key questions with regards to CCTV ï the original reason for implementation and the question of effectiveness. The issue of space is yet again the key to understanding narratives on video surveillance. In this case, the use of the cameras is reasonable in private spaces but not in spaces that, as she puts it, ñbelong to citizensò. Given that space seems to be central in the majority of the statements, we will focus on citizensô attitudes towards the use of video surveillance in the public realm in the following chapter.

3.2.4 CCTV in public space

As stated in the introduction, the location of cameras plays an important role in terms of acceptance. The comparative study UrbanEye has shown that, despite crucial socio-cultural differences, people are more supportive of CCTV in publicly accessible spaces. In the context of our research, CCTV is seen as a ñgood thingò by the majority of respondents, especially in spaces such as ñbanks, stations, platforms, shops, shopping malls, along motorways and in open streetsò[124] as opposed to spaces that are considered more intimate. However, attitudes towards video surveillance are contingent upon culture and situations, such as specific security problems that are contextually addressed through CCTV.

In the context of this chapter, the analysis focuses on narratives on the use of surveillance cameras in the public realm with the aim of understanding how the trade-off between security and privacy is framed when people contemplate technologically mediated control. Do people have a reasonable expectation of privacy in public spaces or do they rather think that the erosion of privacy is less important than security? The following quote seems to shed light on the ambiguity of feelings towards this argument:

> ñ*Personally, I donôt care, letôs put them everywhere! We can talk about privacy in our houses but it is different outside. A soon as we reach the street we are controlled by other people and we lose our privacy automatically anyway. So I donôt see a difference between situations when I am stalked by camera or by people on the street. However, I donôt think that cameras help. Anyone who wants to do something, he does it anyway. It can prevent small criminality but it definitely doesnôt help to reduce serious criminality. It can be used as a tool to solve an already committed criminal act but not to prevent the crime itself. I do notice the cameras when I am in the town. Sometimes, I do modify my behaviour when I know about the cameras appearance and I intentionally avoid the places with them. Even though I am seen I donôt have to be seen by everyone.*ò
>
> (Interview ID 679, 24 years, male, Slovakia)

This account points to several interesting dimensions. Initially, the issue of private *versus* public spaces seems to determine the attitudes towards surveillance cameras. The respondent thinks that CCTV should be ubiquitously used and that privacy is not an abstract idea but rather a *condition* reliant on situations, in particular, privacy depends on where we are. People are entitled to have an expectation of privacy within their homes, but as they enter into public space (ñthe streetsò), privacy is lost. He then uses quite a strong verb to describe the way in which one is controlled either by human or by electronic eyes: there are no differences, in his account, between being *stalked* by technology or by people. The narrative turns to what we previously defined as the objective dimension of CCTV that is, the use of surveillance cameras from a security perspective. Yet again, cameras are considered of little help as far as crime prevention is concerned but they can be useful in criminal investigations. Perhaps the most important statement comes at the end of the quote, where the ambiguity is most

[124] Hempel, Leon and Eric Toepfer, *CCTV in Europe. Final report*, Working Paper No.15, Centre for Technology and Society, 2004, p.43 http://www.urbaneye.net/results/ue_wp15.pdf

apparent. While initially the respondent is fervently in support of video surveillance, he then goes on to claim to avoid places with cameras and to change his behaviour if CCTV is in operation.

On the one hand this story confirms what has been discussed in previous sections, in particular the difference between objective and subjective ideas on CCTV. On the other hand it draws attention to a ñdilemma within the dilemmaò, namely visibility *versus* invisibility for which no clear-cut views seem to emerge. The trade-off between security and privacy depends on spaces (public and/or private), but it is seen critically as the respondent negotiates visibility. In other cases, negotiation is not even taken into account, as the use of CCTV for security purposes in public spaces is not questioned because ñsurveillance is there for a good reasonò. It is difficult to identify trends within the interviews, as feelings are diverse and sometimes conflicting. When respondents are aware of specific cases that have been solved with the help of cameras in the public realm, then privacy is considered irrelevant and CCTV is viewed as ña good thingò or as unavoidable. If it helps catch the ñbad guysò, privacy is not a concern. It seems that when citizens have a reason to believe that cameras are helpful, other arguments are not raised.

There are certain, specific places within the public realm, which were referred to in the interviews. Public transport, for instance, is considered more vulnerable than other locations and respondents sometimes refer to deviant acts occurring, for instance, on the subway. Yet opinions on surveillance cameras in these locations are divergent. A direct link between surveillance and security is only made if the respondent is aware of a specific fact/crime that has occurred.

> ***ñ****I do support CCTV on the subway. Since there was this rapist on the subway last winter I always have a look if there is CCTV operating. Especially the new ones with the 360 degree vision are excellent. Especially during the night time CCTV is perfect, nothing can happen then****ò***
>
> (Interview ID 517, 21 years, female, Austria)

This respondent feels protected by the cameras: the powerful vision of CCTV prevents violent crimes from occurring on the subway. Her views are very straightforward since she claims that nothing can really happen in an area controlled by cameras. In contrast to the previous quote, the dilemma is non-existent here as she wants to be seen and even actively looks for cameras, in order to feel safer. She ñtrustsò the tool to the point that she does not raise any concerns whatsoever. This exception seems to reinforce our hypothesis: surveillance is welcome if it perceived as effective ï independent of empirical evidence. The priority is security (or the feeling of being safe) rather than potential breaches of privacy. In this case we do not know whether the rapist was caught thanks to CCTV, but we know that this young woman thinks that cameras are ideal tools (the vision is *excellent* and *nothing* can happen). It is worth mentioning that gender might affect opinion on cameras, especially when talking about specific places at particular times (subway at night). Another aspect of this story highlights the role of media in the public debate about surveillance measures. Only a few months before this interview was recorded three women of the same age as the respondent where molested in a subway line running through the outskirts of Vienna. In response, the

free tabloids, which are available at subway stations in Vienna, were campaigning for several weeks to install more CCTV on subway trains. In fact, the rapist in question attacked his victims outside the trains on their way home. The general public was demanding to install more cameras in trains but not in public space.

Narratives on the use of cameras in publicly accessible areas are diverse and do not allow for generalizations. However, we might argue that ï as mentioned above ï conditions and experiences play a role in determining support. Additionally, levels of awareness pertaining to the presence of cameras in public spaces seem to be high. A number of respondents are aware of the location of cameras and consider them legitimate for security purposes.

3.2.5 Absences

During the analysis of our data, we were struck by significant absences. Certain aspects of video surveillance were rarely discussed or raised. Although these missing aspects might be a result of the questions posed, it might also be that our lay-person respondents did not consider certain features important enough to be mentioned during the interviews. Rather than suggesting simplistic explanations, we would like to draw attention to these absences and consider them as missing narratives, which, conversely, are of great relevance in the literature. The subject of smart surveillance cameras, for instance, was barely mentioned during the interviews. When prompted on video surveillance, respondents seem to have the basic version of CCTV in mind with rare instances of precise identification, such as biometrics. This form of contemporary governance[125] does not occur in citizensô discourses on surveillance cameras. The same holds true for the issue of data matching, as respondentsô concerns on gathering visual images and then matching those images with other data was rarely mentioned. Thus, everyday encounters with cameras are perceived as encounters with a technology which is considered as ñstandaloneò and, perhaps, less high-tech than others. Terminology is important to highlight absences: for instance, the word ñprofilingò is neither used nor is it conceptualized by referring to targeting on the basis of appearance. As shown, while discourses on CCTV are not generic, they are framed as if video surveillance were rather unsophisticated. Narratives are more imbued with ñgut feelingsò of being spied upon by electronic eyes, than with feelings of being watched by smart technologies whose data can easily be merged with other pieces of information.

There are also settings or locations missing in the interview. Citizensô perceptions of CCTV are shaped by urban experiences, from shopping to getting from one place to the other. As has been mentioned, public transport is one of the locations where CCTV is probably more apparent while other places, such as banks or motorways are often not taken into account. Surveillance cameras are understood to be embedded features of urban contexts and different locations are rarely considered.
Whilst refraining from suggesting reductive interpretations, we argue that missing narratives are worth pointing out as they may point to what lay-people do not consider and consequently emphasize a deeper understanding of how surveillance is really perceived in relation to mundane activities.

[125] Ajana, B., *Governing through Biometrics. The Biopolitics of Identity*, Palgrave Macmillan, 2013.

3.2.6 Concluding thoughts

Our analysis shows a number of distinctive elements. Whilst the following cannot be generalized, they can certainly contribute to the rich debate on citizensô views on surveillance. In particular, our respondents drew attention to these factors:

- The normalisation of (video) surveillance is often questioned through narratives that revolve around issues of a false sense of security and asymmetries of power;
- The feeling of ñbeing watchedò has significant consequences which range from direct impact on behaviour to the production of ñdocile bodiesò;
- People do not simply comply with the fact of constantly being ñspied onò or visible;
- The gaze of CCTV is inevitable but there are options for resilience;
- When it comes to thinking about cameras at an abstract level, the dilemma of security *versus* privacy is not of particular significance. If CCTV is used for security reasons, it is accepted and welcomed;
- The overall security approach behind the use of cameras is often questioned as is the usefulness of surveillance cameras (especially on how the footage is used) as tools for crime prevention;
- Feelings towards the use of CCTV in public spaces vary from acceptance to privacy concerns. Specific conditions and personal experiences play an important role in determining support.

As we have demonstrated, citizensô attitudes are far from unproblematic and cannot easily be dismissed through the notorious ñnothing to hide, nothing to fearò argument. The steady proliferation of surveillance cameras in Europe has not led to CCTV being uncritically accepted. The emerging picture is multi-layered and brings social and legal concerns to the fore.

3.3 PREVENTING CRIME AND VIEWS ON SECURITY IN A CHANGING SOCIETY

Martin Kovanič

Provision of security for its citizens is traditionally understood as one of the main functions of states. In todayôs world, which is considered to be increasingly unstable and insecure, the installation of various surveillance mechanisms is a common answer to these perceptions. The area of security has experienced a fundamental shift in our societies. With their move towards post-modernity, socio-economic changes brought an increased sense of insecurity in societies, which reacted with a focus on management of risk[126]. Combined with technological revolution and the development of surveillance technologies, the ways in which order is created and maintained changed essentially[127].

The reliance on traditional policing mechanisms, such as community patrolling and face-to-face surveillance gave way to the use of more sophisticated technologies, which enable the

[126] Lupton, Deborah, *Risk*. Routledge, New York, 1999.
[127] Ericson, Richard V., and Kevin D. Haggerty, *Policing the Risk Society*. University of Toronto Press, Toronto, 1997.

monitoring, collection and processing of information in order to come up with a set of pre-emptive activities. The temporal orientation is towards the future ï identifying crime before it even happens.

9/11 was a paradigmatic event, which brought a change in the perception of surveillance technologies and practices in connection with security. It brought about widespread acceptance and normalisation of surveillance. Lyon argues that ñit is possible that on a simple calculus, citizens accept that loss of privacy is the price to be paid for security.[128]ò This was reinforced further by subsequent terrorist attacks and the ñwar on terrorò, which facilitated the implementation of various surveillance technologies that aim to increase public perceptions of safety.

The main purpose of this subchapter is to inspect the relationship between security and privacy. Moreover, we are interested in identifying citizensô views on the functioning of various surveillance mechanisms used to prevent crime and increase safety in public spaces. Simultaneously, we are interested in peopleôs strategies to protect their personal property. This subchapter focuses on surveillance mechanisms other than CCTV cameras, which were the main focus of the previous subchapter.

The central concept of this chapter is fear of crime, or feeling of insecurity, which affects the respondentsô attitudes towards surveillance. Fear of crime has become one of the major issues in todayôs societies. Research in the UK however, has shown that there is a gap between actual crime and perceived crime.[129] The fear of being victimized is higher than the actual threat. Nevertheless, fear of crime is an important factor, which needs to be taken into consideration. This can be illustrated by statistics in our respondentsô countries of origin.

In the UK, the fear of crime level is one of the highest. A survey showed that 33.7% of British citizens feel unsafe or very unsafe in public spaces after dark. The highest levels of insecurity are in Slovakia ï 39.7% of Slovak citizens. In Germany, it is 24.8% of citizens. The lowest levels of fear of crime are in Austria ï 17.7% of citizens[130]. These figures confirm that this is a relevant concern of European citizens, especially in the UK and Slovakia.

On the other hand it should be noted that violent crime in general is declining in the countries studied. This fact is illustrated by the following table. Although statistical evidence in the field of crime is only of limited value, it can, however, demonstrate general trends.

[128] Lyon, David, "9/11, Synopticon, and Scopophilia: Watching and Being Watched", in Kevin D. Haggerty and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006, pp. 35-54.
[129] Mirrlees-Black, Catriona, Pat Mayhew, and Andrew Percry, *The 1996 British Crime Survey. Issue 19/96*, Home Office Statistical Bulletin, Research and Statistics Directorate, London, 1996.
[130] The survey was carried out in 2010, it is taken from Hummelsheim, Dina, Helmut Hirtenlehner, Jonathan Jackson, and Dietrich Oberwittler, ñSocial insecurities and fear of crime: a cross-national study on the impact of welfare state policies on crime-related anxietiesò, *European sociological review*, 27 (3), 2011, pp. 327-345.

	Violent crime instances						
	Year	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**
Country	**Italy**	136 322	145 209	153 997	146 598	131 610	127 736
	Austria	42 928	43 316	46 217	47 034	47 602	44 618
	Slovakia	13 575	11 584	10 274	9 669	8 963	8 094
	Germany	212 832	215 471	217 923	210 885	208 446	201 243
	England and Wales	997 159	972 283	885 718	839 323	827 122	795 615
	Scotland	26 558	27 618	25 182	24 777	21 662	21 499

Statistics taken from EuroStat - Crimes recorded by the police[131]

Although this table only deals with violent crime, it can be seen that generally figures are on the decline. However, as already mentioned, the fear of crime itself, whether justified or unjustified, should be taken into account, because it has an effect on individualsô perceptions of security.

This section will be divided into three main parts. In the first part, we will analyse the fear of crime itself, the way it is constructed, as well as respondentsô individual strategies to overcome this problem. The second part will discuss crime prevention in public places ï from the perspectives of the watched and the watchers. A typology of citizens and their attitudes towards public surveillance will be created based on the stories analysed. Moreover, this will include the perspective of law enforcement on the use of surveillance for the purposes of crime fight. Although this was not envisaged in the research, which is mainly focused on citizensô perspectives, a number of interviews were conducted with law-enforcement agencies, which provide a supplement to the analysis of attitudes towards surveillance in the context of security, also touching on the issue of privacy. The last part will deal with property protection and attitudes towards the processes of privatization of security and the growing responsibility of individuals to provide for their own safety

3.3.1 Fear of crime

Fear of crime is a feeling of insecurity in citizensô lives, which influences their behaviour in both public and private. It can be influenced by many factors and it affects various groups of people in different ways. Fear of crime can have negative social ramifications ï it can lead to increasing isolation of individuals and withdrawal from ónormalô social life, as well as growing mistrust in authorities, which are supposed to provide security and the feeling of safety[132]. The existing research shows that fear of crime is higher among women and citizens of higher age, although the age factor has been challenged[133]. The distribution of changes in

[131] Eurostat, *Crimes recorded by the police.* Accessed on http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=crim_gen&lang=en, 08 Jun 2014

[132] Review of Scientifically Evaluated Good Practices for Reducing Feelings of Insecurity or Fear of Crime in EU Member States, European Communities, 2004. http://www.eucpn.org/pubdocs/review_reducing_feelings_insecurities_fear_crime_en.pdf

[133] Lagrange, Randy L., and Kenneth F. Ferraro, ñAssessing Age and Gender Differences in Perceived Risk and Fear of Crimeò, *Criminology*, vol. 27, 1989, pp. 697ï 720.

the levels of insecurity are also spatial, the highest levels are usually connected with town centres and deprived neighbourhoods.

High levels of insecurity are a precondition of the proliferation of surveillance in the context of crime fight. It is the most commonly used justification for the implementation of more surveillance, as well as the introduction of new technologies, which can help to decrease crime rates. This claim ï that fear of crime leads to calls for more surveillance ï is one of the overriding themes of this subchapter. In this section, we show that citizens, have different rationalizations of their fears of crime and causes of security problems.

The stories of fear of crime can be divided into two categories. The first category is the *fear of crime based on experience*. Here, the justifications are based on either personal or mediated occurrence of crime in the areas, where respondents live or spend their time. The second group is *constructed fear of crime*. In this case, the crime was not personally experienced, but it is a result of oneôs beliefs and prejudices. First we will analyse the experience-based fear of crime, which can be illustrated by the following story:

> *ÄYes, I talk about crime with my neighbours, as all my neighbours have been victims of burglaries, I have been victim of an attempted burglary, but they succeeded only in breaking a window, but I came back home after just 15 minutesé I was so angryé I immediately asked my daughter to close the gate and I went out, as I saw two guys passing by I simply shouted that the police was coming and they didnôt reply to me obviouslyé I think that technical or technological measures are useless, my neighbour who has been victim of burglaries three times, has bars to her windows but I think they are useless systems of preventioné nobody has installed alarm systems.ò*
>
> (Interview ID 208, 62 years, female, Italy)

The feeling of safety of the respondent was changed by her neighbourôs personal experience with burglary, which altered the previous feeling of safety. This feeling of insecurity does not lead to direct calls for more surveillance in the area. People who experienced crime often have similar opinions, which are also connected with implicit distrust towards the authorities ï the police ï who in their views do not do enough for crime prevention. Therefore there is a need for people to take matters into their hands and take the initiative in providing their own security. This is something we will address in a later section.

The second category, the constructed fear of crime can be illustrated by the following quote. This story is from Austria, a country that has rather low crime levels, and therefore is an example of the gap between perceived and real crime levels, referred to above.

> *ñI used to compare the EU always with our Monarchy [Austria, Habsburg monarchy], it wonôt work. The EU destroyed the surveillance we already had in this country; that surveillance was good and it worked. The EU took away the security and the strict control over the borders every single member state had. The EU did not offer any compensation for that act. The EU acted like a slob who says Iôm going to destroy all the infrastructure all the possibilities we had to fight crime in our countries. I destroy everything, just in case. Now everything is ruined and destroyed by the EU but nothing*

was offered as compensation. A system that really works. I mean (voice gets louder) that canôt be the consequence, first destroying everything and then offering nothing. There are crime tourists and other things like that. The EU offers nothing to fight these people. Iôm not on my own with this opinion, believe me. There are many out there who are thinking the way I do and therefore I stand for a community that is informing and defending itself, more or less.

(Interview ID 359, 69 years, female, Austria)

This story illustrates an opinion ï a belief or prejudice ï that is not grounded on either personal experience, or in statistical data. The respondent clearly identified the actor, which is responsible for the rise of insecurity (the European Union), which resulted in the abolishment of internal border controls within the Schengen zone. This caused the inability of nation states to thoroughly control the movement of people across their borders. It led to the abandonment of working surveillance mechanisms ï border control ï and to the influx of ñcrime tourists,ò in other words individuals who come to the country with the objective of committing crime.

The response to this situation is an increase in surveillance, or more specifically the reinstallation of previously functioning surveillance mechanisms. This reinforces the hypothesis that the feeling of insecurity leads to demands for more surveillance, thus creating a rather paradoxical situation in connection to the relationship between resilience and surveillance. In the society, where the levels of fear of crime or insecurity are rather high, the response of the society to decrease these levels and create a secure environment, is to install more surveillance. Therefore, in this context, resilience of the society is equated with increased surveillance. For the **insecure citizen**, the existing network of surveillance means that s/he can feel safe ï in relation to moving through public spaces, as well as in connection to the protection of his/her personal property. Surveillance is the means with which such individuals can adjust to the changing environment in which they live, which they consider to be increasingly more insecure. In this sense surveillance is resilience: a way to adapt. Rather than just adapting to living in society in which they are surveilled more ubiquitously, this actually forms part of the resilience strategy of certain groups of citizens.

The call for more surveillance is not the only result of the existing fear of crime among the respondents. There are various strategies people apply when dealing with the feelings of insecurity, especially when moving through an area that is perceived as high-risk. The following stories illustrate such tactics:

ñI also lived on the óGürtelô [ring road in Vienna], and there I felt really safe, because of the large amount of prostitutes standing there. So no matter what time you got home, there were people on the street. This gave me a feeling of safety, it was illuminated, also with the clubs and the brothels.ò

(Interview ID 537, 34 years, female, Austria)

The story shows that people are aware of their surroundings, which can be used to increase their feeling of security and lower the fear of victimization. This applies to both physical surroundings (such as the existence of bars on the streets where they walk), as well as pedestrianisation of the area ï meaning presence of the people who can see them (prostitutes

on the streets). This shows that certain individuals do not always trust technology, such as CCTV cameras, but prefer face-to-face surveillance, a chance to be seen by somebody else in case they feel insecure. This to some extent corroborates Dittonôs research, which showed that CCTV cameras are trusted more in relation to detecting and solving crime, but are not as effective in making people feel safer. To increase the feeling of security, people prefer physical oversight, such as more policemen in the streets.[134]

3.3.2 Preventing crime in the public space

Crime prevention in public places has many faces and makes use of many technologies, which fall under the umbrella term of new surveillance. Moreover, technological progress has resulted in the availability of various technologies to make public places safer. These new technologies ï including biometrics and drones ï however raise concerns of privacy infringement, thus creating a dilemma of whether their use can be justified. Again, CCTV will not be discussed in this subchapter. In this section, we are going to present the views of our respondents concerning crime prevention in public spaces and a plethora of reactions towards these issues. It will be divided into two main parts ï perspectives of the watched and the watchers.

The Watched

The first section focuses on the reactions from the point of view of the watched ï individuals who move through public spaces and either engage with the existing surveillance technologies, or present their opinions about their use. In general, people are aware of the existence of these technologies and they have adjusted to living with them as they engage with them on a regular basis. This is especially evident in specific surveillance sites, such as airports. Security checks at the airport epitomize the use of surveillance for the purpose of crime prevention, since engagement with them is very physical and very real. Therefore this is something mentioned in a number of the stories analysed. Although we can claim that these security checks are in general accepted ï and hence surveillance is normalized ï the reactions of the respondents varied.

The first type of reaction is complete acceptance of the measures, in order to be secure. This approach is demonstrated by the following story:

> *ĂIf you think about America where you need to strip off your clothes more or less before [you enter the country] nowadays. The advantage is that I enter the country in 5 minutes today because they have already everything on the screen. They take your picture and finger prints and thatôs it. (é) I accept the checks/controls, because - in the end ï reason tells you I prefer to be checked and not to explode when somebody smuggles something into the airplane. At the same time, you know that a lot can be smuggled in nevertheless.ò*
>
> (Interview ID 52, 55 years, male, Austria)

[134] Ditton, Jason, "Crime and the city: Public attitudes towards open-street CCTV in Glasgow", *British Journal of Criminology*, Vol. 40, No. 4, 2000, pp. 692-709.

This type of respondent, the *accepting individual*, sees the existing surveillance in public places as something necessary, even advantageous. Endorsing the ñnothing to hide, nothing to fear mentality,ò the existence of large amount of data is seen as favourable, since it enables him/her to pass along the surveilled entrance (in this case it is a security check at the airport) without need for any further control. He voices no concerns about the loss of privacy ï security is ña right,ò which is important and which can be achieved through surveillance. The type, accepting individual, confirms the hypothesis that people always choose security over privacy.

This particular case also shows another recurring theme, which is the effectiveness of surveillance in relation to the provision of security (which is something often connected to CCTV surveillance). This particular concern was raised by a plethora of respondents, especially pertaining to airport security. This is to some extent a paradoxical situation, since airport security checks are allegedly very careful but on the other hand, respondents still have doubts whether they are thorough enough, when it comes to looking for liquids and sharp objects. Therefore one of the main concerns does not address the infringement of privacy, but the ability of surveillance to function properly and effectively.

The second type of respondent, the *conscious individual,* accepts surveillance, but has certain reservations towards some of the measures. S/he voices some privacy concerns and thinks that there is a need for certain ñboundariesò, even when it comes to security. This is illustrated by the following story:

> ***ñ****I do think the safety controls are ok. But I'm not in favour of the liquid regulations [at airports] because people are thirsty and they need something to drink. I think naked scanners are not necessary and they are violating privacy. And I am also against recordings, taking pictures, and finger prints. The controls in North America are annoying. In Vienna, it's still not too bad.**ò*
>
> (Interview ID 386, 24 years, female, Austria)

Although the surveillance mechanism is accepted in general a concern for the existence of boundaries is clearly voiced. The respondent is particularly against the introduction of new surveillance technologies ï such as full body scanners and biometric fingerprinting ï that are considered too pervasive. The reaction to the introduction of such technologies is a demand for stricter regulation. The same line of argumentation can be seen in the some of those stories that are normative, not based on experience. Introduction of new technologies such as drones, or biometric databases is considered a development, which could help fight crime, but conscious individuals also think about possible threats of misuse.

Another problem voiced by the conscious individual is function creep. The respondent accepts the existing surveillance measures, which have their functions. However she is also aware of the fact that many technologies, which were designed for fighting crime and the provision of security ï such as ANPR ï are being used for other purposes as well. Function creep is seen as one of the biggest problems and the reflective individual opposes it. This results in the aforementioned call for more regulation. The problems of function creep are compounded by the fact that the consequences and possible threats of new surveillance are

not always carefully contemplated ï even by the people responsible for approving their implementation.

The final type is the *antagonist*, an individual who opposes the existing surveillance measures. This results either in surrendering to the situation or a conscious action ï such as avoiding the surveillance. This approach can be identified in the following quote:

> *ǍIt is about connecting data about certain persons from different sources. I have a problem with this. See at the INDECT-Demo, the police filmed us, almost close-ups, if they cut out single pictures and then use face recognition technologies to find me on Facebook and see: Uh, he's received jobs from the "civil service", then maybe this information could be passed? I am not thinking that this is paranoid, but I have become more cautious.ò*
>
> (Interview ID 35, 60 years, male, Germany)

This type of respondent is aware of the existing surveillance, as well as of its possibilities. He is aware of the amount of data that exists in databases and sees this as a breach of privacy. Some of the accounts of antagonists draw a parallel between the functioning of modern societies and Orwellôs dystopia. The 9/11 attacks are identified as a breaking point, which enabled the introduction of excessive surveillance and control. This particular account shows an antagonist, who is trying to take a conscious action ï being more careful when moving through public spaces, especially in the context of specific events, such as demonstrations. The respondent voices concerns of being identified when attending these kinds of events, so in this sense surveillance is an obstacle in exercising basic human rights and freedoms.

Antagonists suggest that we are living in the society of presumption of guilt ï they emphasize ñfeeling like a criminal,ò when having to engage with existing surveillance systems. They clearly oppose the introduction of new technologies for surveillance purposes (such as INDECT). Another example of resilience by the antagonist is to avoid flying whenever possible, in order not to have to go through security checks.

The watchers

Some of the interviews concerning crime prevention were also conducted with experts ï representatives from different law enforcement units. Therefore in this section, we present the perspective of the watchers as explained by the watcher themselves. Roy and McChaill suggest, that our societies underwent a paradigm shift towards risk-based strategies of social control, which has implications for criminal justice. This shift towards the new penology changed the focus from individualised suspicion towards risk assessment of potential criminal behaviour[135]. In order to be able to do this, law enforcement needs large amounts of data and consequentially takes advantages of various mass surveillance technologies.

The empirical material collected for this part of the IRISS project highlighted, that this is indeed the case. Law enforcement agents confirmed that they make use of a variety of information ï ranging from tracking cell-phones, through Electoral roll in the UK to making

[135] Coleman, Roy and Michael McCahill, *Surveillance and Crime*, SAGE Publications Ltd, London, 2011, pp. 69-70.

use of various databases such as Trace IQ[136]. However use of surveillance technologies is not straightforward and does not always produce a definite answer. This experience is illustrated by this example:

> *ñSo this pantechnicon is not all-seeing and embracing, and we relyé Like this public domain, I can find the quotation for you if necessary but I canôt remember the exact figure, but itôs something like 80% of the plots in Western Europe have been identified through electronic surveillance, the original catalyst to start the investigation, which obviously now we know after what Snowden and Prism allege makes a lot more sense. But exchange of emails or whatever, somebodyôs gone and referred it through to the Security Services, who then have done their own work and decided yes or no, or we think itôs a runner, and then itôs passed out to the catch territory to look at, or we think you should do something about this. And then you start on your focus rather than just putting out a call.ò*
>
> (Interview ID 387, 60 years, male, United Kingdom)

This story clearly shows that surveillance ï in this case electronic mediated surveillance ï is an integral part of the risk-based approach. It serves as an initial catalyst; it can help identifying the possible threat. However the next step is going back to traditional policing techniques. Technology alone does not catch suspects. Therefore there is a need to go back to individualised suspicion, which is a characteristic trait of old rather than new penology.

One of the issues law enforcement units face when accessing private information of possible suspects or persons of interest, is data protection. Naturally, some of the databases cannot be accessed without a valid judicial order. One of the stories deals with such a database and offers a strategy of how to bypass the need for official order.

> *ñThere's a way, if you're in the tax office, if you're at your terminal, if I search for you, there's a record ï or my understanding of it when he was telling me ï there'll be a record that I have searched for you. Now, if I do a general search for all the people that share your name or what sounds like your name, there's no record that I've searched you. But what I can do is I can go down the screen and it'll just go through all the people with your name on it. Now, if I look into your folder ï again, there's a record kept that this individual has looked at your folder. So what they do is, as they're going through the screen, they just do a screen grab of what's there, and that gives you the last three years. So it's your name, your address, national insurance number, what your tax code is, who you work for, how much tax you've paid over the last three years and what your income's been. What they give is a screen grab and then there's no reference that that search has ever taken place.ò*
>
> (Interview ID 403, 50 years, male, United Kingdom)

Although there are some regulations in place, there is usually a way to avoid them and to make use of existing surveillance infrastructure. This is in accordance with the belief that

[136] These are web-based tracing and investigation facilities, see more at eg. http://www.tracesmart.co.uk/

criminals can always be one step ahead of the police, since they do not have to follow any regulations and therefore the police have to react accordingly.

Law enforcement agencies are aware of the fact that you cannot always trust the information collected by various surveillance mechanisms. Criminals are also aware of them and they come up with their own avoidance strategies. The case of the planned English Defence League rally bombing is mentioned:

> *I suppose if youôre talking about digital surveillance, itôs just simply it could be recorded. I donôt think weôve got a hedge round that yet as a society where you leave a magical digital footprint. But criminals and aspiring terrorists know theyôre vulnerable by leaving a digital footprint, and they will take fairly simple steps to ensure that their digital footprint isnôt there, or itôs much reduced. So Iôd have to look it up, but itôs in the public domain, the arrests of the guys from Birmingham who went to Dewsbury to attack the whole process, they didnôt have a phone with them. They had left their phones at home. Now the very nature of leaving your phones at home, if they had been under surveillance and they were not, then nobody would know whatôs going on, but they left their phones at home, and thatôs the simple thing to do.ò*
>
> (Interview ID 384, 60 years, male, United Kingdom)

This case is a fairly controversial one, since it illustrates the failing of the existing surveillance network ï police and security services had no intelligence about the plan although one of the perpetrators was under surveillance due to being a suspect in a different case. However, they were caught by a different surveillance network ï ANPR ï which identified that their car had no insurance and were then stopped by the police[137].

Perpetrators in this case were aware of the surveillance possibilities and therefore left their mobile phones at home. This again is an example of resilience, from the point of view of criminals. A high level of awareness of the surveillance potential of various technologies leads to conscious strategies of avoidance.

3.3.3 Property protection

In this section, we will turn to crime prevention in the context of private properties. The working hypothesis of this subchapter is that when people feel insecure they do not rely on public authorities, but rather they try and take care of their property themselves. The underlying argument can be found in theory. In todayôs societies, ñresponsibility for security is being distributed to individual citizens, or insecurity subjects, to ensure their own safety through consumption.[138]ò This can be achieved through various means ï either increased protection of oneôs property with technological systems (such as CCTV, alarm), or living in gated communities with a private security service.

[137] For detailed information about the case see http://www.bbc.com/news/uk-22344054
[138] Monahan, Torin, *Surveillance in the Time of Insecurity*, Rutgers University Press, New Jersey, 2010, pp. 81.

However, the notion that individuals are responsible for their own security is not straightforwardly accepted. The following quote illustrates the line of thinking about the relationship between public and private security provision:

> *ñItôs complicated. On the one hand protection is traditionally a function of the national state, and actually one of its main legitimacies. But the public is asking for more and more protection all the time? Really? On the other hand of course you have to take some minimal care yourself. Burglary exists in a society and you have to take care - if you leave the house door open most likely your bike will be gone from the backyard.ò*
>
> (Interview ID 987, 44 years, male, Austria)

The belief that individuals have a co-shared responsibility when it comes to protecting their property is shared among the respondents. However, as can be seen in this response, the delegation of security to individual citizens is not fully accepted. The provision of security by public authorities (in this case the nation state is mentioned) is seen as one of their fundamental functions, although the respondent expresses the view that public demand can never be fully satisfied.

The need of individuals to perform some extra activity in order to secure their property is clearly linked with the feeling of insecurity, something that is often connected to the perceived security of the neighbourhood, where the individual lives. This means that the **secure citizen** does not have the need to employ any additional precautions:

> *ñPersonally, I havenôt taken any measures to prevent crime and I wouldnôt use anything to protect me from burglary as I feel safe only when I am open to society. However, this depends on the context. I live in a small city. We watch over each other's apartment. There are 36 families in my condo, twice a year we have a big lunch all together and this makes a difference, I think. Nothing has ever happened. Never. The logic is: building relationships of trust with neighbours. We donôt ask people who come to visit other people in my condo to show their IDs! He or she is someone's guest. This someone takes responsibility for his/her guest.ò*
>
> (Interview ID 1, 70 years, male, Italy)

The decision to take extra security precautions is a rational calculation. It has certain costs ï financial as well as time, although in this case there are no privacy considerations since the system is operated by the same individual, or family members ï and benefits ï the increase of security. If the security level is high (living in a good neighbourhood, as compared to others, where crime levels are higher), then the costs are high. However, even when the respondent claims that s/he is feeling safe, the cost-benefit analysis leads to the introduction of some low-cost solutions ï such as installing lights next to the front door, or having a more sophisticated security lock.

Another cost, which was mentioned in several interviews, was the value of an individualôs property. An approachï *ñI have nothing valuable, therefore I do not need any extra protectionò* ï was mentioned by several respondents. In contrast, when somebody has

advanced security measures in effect, it might suggest that his/her property includes valuable items.

On the other hand, for the *insecure citizen* the cost-benefit analysis leads to the decision to employ security measures of some kind. These can be either technological (such as CCTV, or alarm systems) or construction-based (such as the installation of more secure doors, windows, lock system). The fear of crime, as we mentioned earlier, is either a direct result of experience, or constructed. An example of experience-based fear of crime can be seen in the following story:

> ñ*The feeling of someone having broken into your home, snooped around in your privacy and opened your drawers. And then the police was also there and just stepped over all my belongings that where lying on the floor. That was really unpleasant. And it damages your safety feeling. Since the burglary happened, I always control my door twice. In the past at the countryside we didnôt lock the door at all, it was open all the time. And I did the same in my apartment. I just let the door fall into the lock. But now, I lock the door, also with a chain, because I know it can be opened really quickly.*
>
> (Interview ID 541, 34 years, female, Austria)

With the experience of burglary, the feeling of security rapidly declined and changed the perception, as well as the actions of the involved individual. In this case the change does not involve a radical introduction of new security measures, but rather that the respondent starts to make use of existing ones. An increased feeling of insecurity leads to the introduction of both construction-based changes (in this case it is the chain on the door), as well as technological ï such as instalment of CCTV (already discussed in chapter 2.3 ñCCTV in Europeò) or alarms and even motion-sensors throughout the house.

3.3.4 Concluding thoughts

The analysis showed that there are various types of people, who interact and react to surveillance in different ways. The attitude towards the relationship between surveillance and security is influenced to a large extent by an individualôs feeling of insecurity. This applies when respondents talked both about movement through public spaces, as well as protecting their private property. Several interesting trends emerge:

- The feeling of insecurity, which can be both experience-based and constructed, has an effect on the perception of surveillance
- The ñinsecure citizenò is more likely to be in favour of surveillance and privacy concerns play a secondary role at best. Surveillance can be considered resilience towards existing insecurity. This is especially true for the accepting individual.
- The ñconscious individualò is aware of surveillance, does not oppose it, but s/he raises the issue of regulation
- There is a type of respondent who opposes surveillance on the grounds of rights violations and modifies his/her behaviour when interacting with the technologies.

- Decisions about measures to protect oneôs property are rational. The level of insecurity, as well as the value of possessions is taken into account.

In conclusion, the attitudes of respondents towards surveillance vary. Although the opposition/resistance towards surveillance is almost non-existent, there are demands for regulation of its use in public spaces by citizens who feel relatively safe. The ñnothing to fear, nothing to hideò approach is only voiced by the insecure individual.

3.4 CONCLUSION

Chiara Fonio, Martin Kovanič

In this chapter we explored the dilemma between privacy and security by focusing on technology. In particular, we drew attention both to a specific surveillance tool (CCTV) and to views on security and crime prevention. In general fear of crime plays an important role in this context. We investigated several dimensions, one of them being the difference between the watchers and the watched and how the latter perceive control through technology. As we showed, several ambiguities seem to arise pertaining to citizensô attitudes towards surveillance technologies. More often than not, citizens do not have clear-cut views, however, there are a few recurring themes which are worth considering.

The dilemma between security and privacy is presented as irrelevant if the respondents have a good reason to believe that security tools ñworkò. Moreover, the general belief is that more surveillance is more likely to increase security. Despite the differences between reality and perceptions, it is worth noting that the latter affects feelings of security and can therefore also play a role in changing the attitudes of citizens who perceive themselves as ñinsecureò or ñat riskò. However, what seemed to emerge are doubts about the effectiveness of technology along with questions on the overall approach to security. For instance, the *delegation of security to technology* was emphasized by many respondents as well as the *false sense of security* provided by surveillance tools. The effectiveness of technology is connected rather more with fighting crime, then with crime prevention. Our interviewees highlighted the importance of personal and/or social responsibilities in order to feel safe and to live in a safe environment.

Privacy is at stake when citizens report personal feelings of being ñstalkedò or ñwatchedò. Surveillance is not always taken for granted, especially in the urban context. Although the ñsurveillant gazeò is not always accepted, the inevitability of surveillance permeates everyday life. Nonetheless, there are options for *resilience*, namely avoiding places where there are a certain number of cameras, for instance, or trying to be ñless visibleò, that is behaving normally when ñspied uponò. However, the notion of resilience appears complex and multi-faceted. Like surveillance, resilience has two faces: one draws attention to options to avoid control, the other is the opposite as resilience can also be surveillance. In other words, *resilience as surveillance* emerges when the feeling of insecurity is prevalent.

Another important insight is the high level of awareness of surveillance technologies. Citizens we interviewed are familiar with the surveillance society they live in and daily encounters

with technology do not go unnoticed. Yet, it is difficult to determine whether awareness relates only to the visibility of security tools or also pertains to a deeper understanding of the consequences of surveillance. Nevertheless, especially when considering new high-tech surveillance mechanisms such as drones or biometrics, ñthe nothing to fear, nothing to hideò approach is not prevalent and respondents implicitly recognize the need for regulation.

To conclude, citizens only rarely use the language of rights violations when it comes to thinking about surveillance in the context of security. Even though the ñgazeò can be uncomfortable and ï as we showed ï might affect behaviour, acceptance towards surveillance in the general public is quite high.

4 3ND DILEMMA: PRIVACY AND SOCIALITY

Keith Spiller

4.1 INTRODUCTION: THE RISE OF THE INFORMATION SOCIETY

The Internet has had a dramatic effect on Europe and the world since the mid-1990s. As we have seen in other chapters it has revolutionized forms of shopping and marketing, as well as intensifying issues of privacy and security. In this chapter the emphasis is on communication or more especially how the Internet has facilitated new and inventive means of connecting people and the emerging socialites that are entwined with this development. How citizens now chat via Skype or write via email have revolutionized the speed and agility of communication. Indeed, less intimate forms of communication ï where contact is not one-to-one and is directed at mass audiences ï have equally opened up new social forms and means of interaction. In these instances, the motivation and appeal is often promotional and opinion driven and this form of communication has been used in ever diversifying contexts. Twitter and Facebook, for example, have the ability to promote new consumer products, academic publications, community events or the comments of journalists and sports stars. There are some distinctions to be drawn here between social network and social media; media is predominately used to speak to larger audiences and, while it can, it is not designed to speak directly, i.e. one-to-one conversation. Social networking, on the other hand, tends to cultivate familiarity through establishing and maintaining friendships or sharing personal pictures and preferences. Other differences include the design and function of sites and the commercial opportunities afford by the platforms.[139] However, one overriding commonality linking much of this activity is the generation of digital and recordable data. In each and every instance, there is a data trail left by users indicating what they are viewing, commenting on and how and where they are interacting with other users. The use of this information has untold implications for surveillance, particularly the harvesting and mining of the information produced. Indeed, as the Snowdon revelations have vividly indicated the value of this information and its use by governmental agencies as well as the private organisations providing services such as the Internet, search engines or email all deliver extensive and intimate details of how citizens live their lives and the activities they engage in.

A growing awareness of the power of the information users provided through their online activities is taking hold. Indeed, due in no small part to Snowden, the use of data and concerns about the data trail have featured in media outlets not commonly associated with focuses on surveillance or privacy. For instance, a recent British Airways inflight publication[140] ï a publication aimed at airline passengers ï ran an article that included details such as, ó63% of UK adults worry about how much personal data theyôve revealed onlineô or ó48% say data privacy is an issue they think aboutô. The growing interest and dissemination of such findings highlight the awareness that users are party to. However, many citizens while enjoying the benefits the Internet extols are at times carefree in the management of personal data ï as we explain in the following section. The focal narrative of this chapter is how some

[139] See, http://www.examiner.com/article/social-media-vs-social-networking-what-s-the-difference http://socialmediatoday.com/SMC/194754

[140] Downer, S. ôUp Close and Personalô, Business Life, British Airways, May 2014, pp 33-38

of these issues of privacy and surveillance are understood, ignored and dealt with in relation to using and socialising on the Internet.

4.1.1 The influence of social media has grown and grown

Depending on the platform used by users the impacts and expanses of social media posts or comments can be widespread. The scale of impact is of course relevant to the person posting, for instance, Barak Obama has over 35m Facebook friends his comments therefore have greater exposure than most. However, posts also have the potential of going viral ï this is where a post is picked by other users and through recommendations its content spreads. One example of this phenomena includes a video clip placed on YouTube with the intention of showing it to immediate family members. Due to the comedy value of the clip it went óviralô and has received over 700 million views.[141] This of course is a relatively harmless example, there are many others where people have found themselves in compromising or embarrassing positions and again the information has gone viral. The propensity with much of the information placed on social media is to have an impact, as well as ease of access for certain audiences.

Early examples of social media were based upon the structure of bulletin boards, where notifications were placed and audiences could respond or comment on notifications. It is the interlinking and bonding of users that expands on the noticeboard format. The *comments*, *likes* and *posts* of users can be interrelated with others who have commonalities or have joined the same pages or web groups. Beginning in 1985 with what is one of the most widely accepted first forms of social networks Well (Whole Earth ðLectronic Link) was effectively a bulletin boards where members could send private messages.[142] The trajectory of online networks then development with sites such as friendsreunited in the 1990s, where member sought and contacted past classmates and friends. These sites in turn developed, for example, MySpace in the 2000s was used predominately by music lovers and to promote music in various guises, as was LinkedIn introduced in 2003 and designed to help business networks and connections. In 2004 Facebook was launched and in 2006 Twitter went live. What these various sites have in common is an embryonic place to share ideas, opinions, information, photographs or music, as well as providing an opportunity to meet and chat with friends and strangers online. The popularity of these sites has spawned new ways of interacting online, for instance, passive observations, where the need to meet face-to-face in order to exchange personal news or stories has been adapted. Commonly, friends and family are up-dated on the activities of a person through posts made on a social media site. This of course is nothing new, as the postcard or photo album, it could be argued provided similar functions, however what is different is the spread and audience of this information provided by the Internet. Who sees can be controlled and curtailed, but for the most part the information is widely available to many viewers and as such, pressing for a sociologist examining such a concept, is how this technology encourages citizens to perform.

[141] http://www.youtube.com/watch?v=_OBlgSz8sSM
[142] http://www.well.com/aboutwell.html

Example of this sort include LinkedIn, which has a business or professional context, where users present profiles related to work experiences and the platforms serves the purpose of job recruiter and business networking opportunity all in one. Again in this instance, users seek to build an online presence, where they óvisualizeô presentations of the self. Equally the geographical location service of foursquare pin-points the live location of users and advertisers and acquaintances are informed of the usersô whereabouts, which could be used to initiate a social meet-up or a sales opportunity. Much of the speed and spread of social media has been aided by the growth of mobile technologies and the growing sophistication of wireless capabilities ï users have the capability of always being óonô. All of these platforms have the potential to expose the lifestyles, preferences and movements of individuals and this in turn presents distinct advantages and disadvantages to how userôs information is exploited.

The premise to usersô interaction on social media is a repository of personal information that is shared to varying degrees with the audience and organisations that use and manage social media systems. Users edit and censor the information they wish to present. Nevertheless much can be inferred or explicitly extracted from user information that is present as a profile. Recent surveillance work on social media has highlighted some on the security and privacy difficulties faced by social media users. Trottier[143] has drawn attention to how users of social media make themselves visible in ways that may not always be clear to the user and indeed their acquaintances or audiences. In commercial terms this information is often used to match consumers with products. The profile, as Gandy,[144] states is the accumulation of information by an organisations or individuals on an individual. Included are all representations of the self,[145] even ones of exaggeration or those removed from certain realities. The blurring of public and private personas extends the complexity of these presentations, as for instance images from a drunken vacation are viewed by the userôs employer; or employers viewing less than polite comments made on Twitter. Online expressions and identities have real and often unforeseen offline social, legal, political or financial impacts.

User profiles and the use of information within these profiles, Trottier suggests, pose four dilemmas. Firstly, as mentioned there is the marketing and monetizing aspect where collected information can be used to profile and target certain audiences. Secondly, police analysis of user information can be used, as was the case in investigating the London riots and in other high profile cases.[146] Here it would seem issues of privacy and covert intension of police forces posing under assumed user identities has questioned the rights of basic civil liberties most especially in relations to the ethical procedures of such policing practices. Thirdly, institutional or organisational management of data has been called into question, most especially after Snowdenôs claims that large online organisations when requested hand over large amount of raw data to governmental agencies.[147] Again issues of privacy prevail. Fourthly, concerns have been raised about self-presentation where users are activating and normalizing online identities, as well as revealing large amounts of personal information - data that may not have been exposed in other circumstances, i.e. work colleagues viewing

[143] Trottier, Daniel. "Social media as surveillance." *Farnham: Ashgate*, 2012.
[144] Gandy Jr, Oscar H. *The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries*. Westview Press, Boulder, 1993.
[145] Erving, Goffman. "The presentation of self in everyday life." *Garden City, NY: Anchor*, 1959.
[146] http://www.telegraph.co.uk/technology/social-media/8723038/Facebook-and-Twitter-to-help-police-track-riots.html
[147] http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

personal images. Other commentators have also highlighted the generational influence of social media, particularly for teenagers,[148] as Boyd suggests, networked publics are how some of the social interactions of social media online spaces are actualized and used. With reference to the now decreasingly popular music site Myspace, Boyd presents a convincing argument of the need felt by teenagers to conform to social norms. Within these online spaces, "everyone is doing it" and therefore if a teenager wants to be popular, informed and fashionable they will participate in this form of communication. Not to do so would lead to a form of exclusion. This statement of course needs to be taken in context, as being part of a collective is highly desirable for some but not all teenagers. Nevertheless, social media provides a platform for communication and socializing that presents a world in which nascent social etiquettes are formed and reformed for young adults. To some degree this is also an exclusive space or one many teenagers are confident that adults, i.e. their parents, are not comfortable in and unlikely to participate. Although as Boyd states when parents do enter this world there is a quandary because if privacy is set high to exclude the gaze of parent potential teenage viewers will also be omitted.[149]

A current popular platform in social media is the micro blogging site Twitter. In this case there is less of a generational gap, for example, many academics have taken to it in order to access new research findings from conferences, and accepted-but-not-yet-published papers, and to hear views of leading academics on current theoretical/methodological/policy-related issues in the field. Indeed, championing the benefits of Twitter some leading academics have blogged about how to use it in academic settings[150]. Twitter limits user's comments to 140 characters; pictures, videos and shared links can also be included. One of the defining features of Twitter is the re-tweet function; found information can be re-posted by the new users.[151] Equally the hashtag function allows topics of information to the easily found and the re-posted with comment; for example, #IRISS included at the end of a tweet would make it straightforward for any Internet user to find and comment on this project. The power of Twitter is far reaching and can have dramatic political implications, as well as impacts on social unrest. Indeed tools such as BlackBerry Messenger were widely used in the London riots of 2011. The encrypted messaging service encouraged the participation of rioters and offered enticement such as "come and get free stuff" in relation to the many sports stores that were raided. Stealing sports clothing was one of the main activities of the riots, nevertheless it was this form of social media that co-ordinated and advertised the activities to rioters. In other highly contentious settings, social media has also contributed to politically motivated events. Social media supported and intensified the political tensions in the 2012 movement for regime change in North Africa. Equally influential in this context was YouTube, as Twitter was used to co-ordinate activities and YouTube presented the happening to wider and international audiences.[152] A critical event in North Africa was the protest of Mohammed Bouazizi which

[148] Boyd, D. "Why youth (heart) social network sites: The role of networked publics in teenage social life". *MacArthur foundation series on digital learning– Youth, identity, and digital media volume*, 2007,pp 119-142.
[149] See, Beer, David. "Can you dig it? Some reflections on the sociological problems associated with being uncool." *Sociology* 43, no. 6 (2009): 1151-1162.
[150] See http://deevybee.blogspot.co.uk/2011/06/gentle-introduction-to-twitter-for.html
[151] Boyd, D., Golder, S., & Lotan, G. (2010, January). Tweet, tweet, retweet: Conversational aspects of retweeting on twitter. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference, 2010* (pp. 1-10).
[152] Eltantawy, Nahed, and Julie B. Wiest. "The Arab Spring| Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory." *International Journal of Communication* 5 (2011): 18.

when reported on Facebook went viral.[153] Moreover, Tunisia, where the Arab spring is credited as starting, had 2 million Facebook users at the time that helped to spread and drive how the event was reported. Twitter, bloggers and Facebook users all carried messages of protest as its profligacy and political impact grew. Indeed, social media users often posted clips of television coverage to highlight the governmental message and itôs, at the time, political leanings.[154] Such clips were used to highlight abuses of civil rights and often resulted in western celebrities posting comments or re-twitting the information.

Much of the power of social media can be understood through the changing elements of the Internet. Being ónô and having instant and 24 hour access to news, blogs and ófeedsô has irredeemably altered the communication landscape. To the forefront has been the use of smart phones or devices, where access to the Internet is available remotely and widely throughout most European countries. Indeed, the use of mobile Internet use has seen a substantial jump in the level of usage, 36% of Europeans in 2012 accessed the Internet daily via a mobile device (smart phone, tablet or PDA (personal digital assistant),[155] whereas in 2011 14% of Europeans did.[156] It is to some of these effects that we turn in developing our argument throughout the chapter. However, we now introduce the 5 focal countries to this report and give some background information on Internet use in these countries.

4.1.2 Focal countries

The five countries from which our data is generated are Germany, Slovakia, Italy, Austria and the UK. As mentioned in earlier chapters these locations where picked to provide an overview of some of the contemporary issues facing Internet usage in Europe. The impact of Internet use and indeed some of the surveillance repercussion felt in Europe post-Snowden has differed throughout Europe particularly in reaction to the security of personal data revelations. This may be related to the rates of Internet use, therefore we provide a short overview here. We limit the detail to percentages of citizens with access to the Internet, average daily use of the Internet and use of social media. All of these results concentrate on our selected countries and on popular social media platforms such as Facebook and Twitter.

Facebook has over 250 million active users[157] and about 347m account holders in Europe[158]. However other platforms widely popular worldwide such as Twitter have proved less successful in Europe, as a recent article stresses, Germanyôs reluctance to use Twitter may have cultural and historical antecedents ï recent histories of state-watching personal communications may make users less likely to volunteer personal opinion.[159] Indeed, some commentators suggest Germans rarely comment online and are passive users.[160]

[153] Khonder, H.H. Role of the New Media in the Arab Spring, Globalizations. Vol 8 (5) 2011, pp 675-679
Beaumont, P. The Truth about Twittter, Facebook and the uprisings in the Arab World. The Guardian, 25 February, 2011.
[154] The liberating quality of the internet has of course been queststioned ï see, Morozov, Evgeny. The net delusion: The dark side of Internet freedom. PublicAffairs, 2012.
[155] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DE%20Internet%20use_0.pdf
[156]http://www.iabeurope.eu/files/3713/6852/4105/european20mobile20Internet20use_executive20summary.pdf
[157] http://www.Internetworldstats.com/stats4.htm)
[158] http://www.insites-consulting.com/347-million-europeans-use-social-networks-results-of-a-global-social-media-study/
[159] http://www.economist.com/blogs/babbage/2013/12/social-media
[160] http://lovable-marketing.com/2013/10/18/twitter-in-germany/ and Insites-consulting.com op cit

Nevertheless, the popularity of other forms of social media in Europe is substantial and continues to expand, as the follow figure demonstrates.[161]

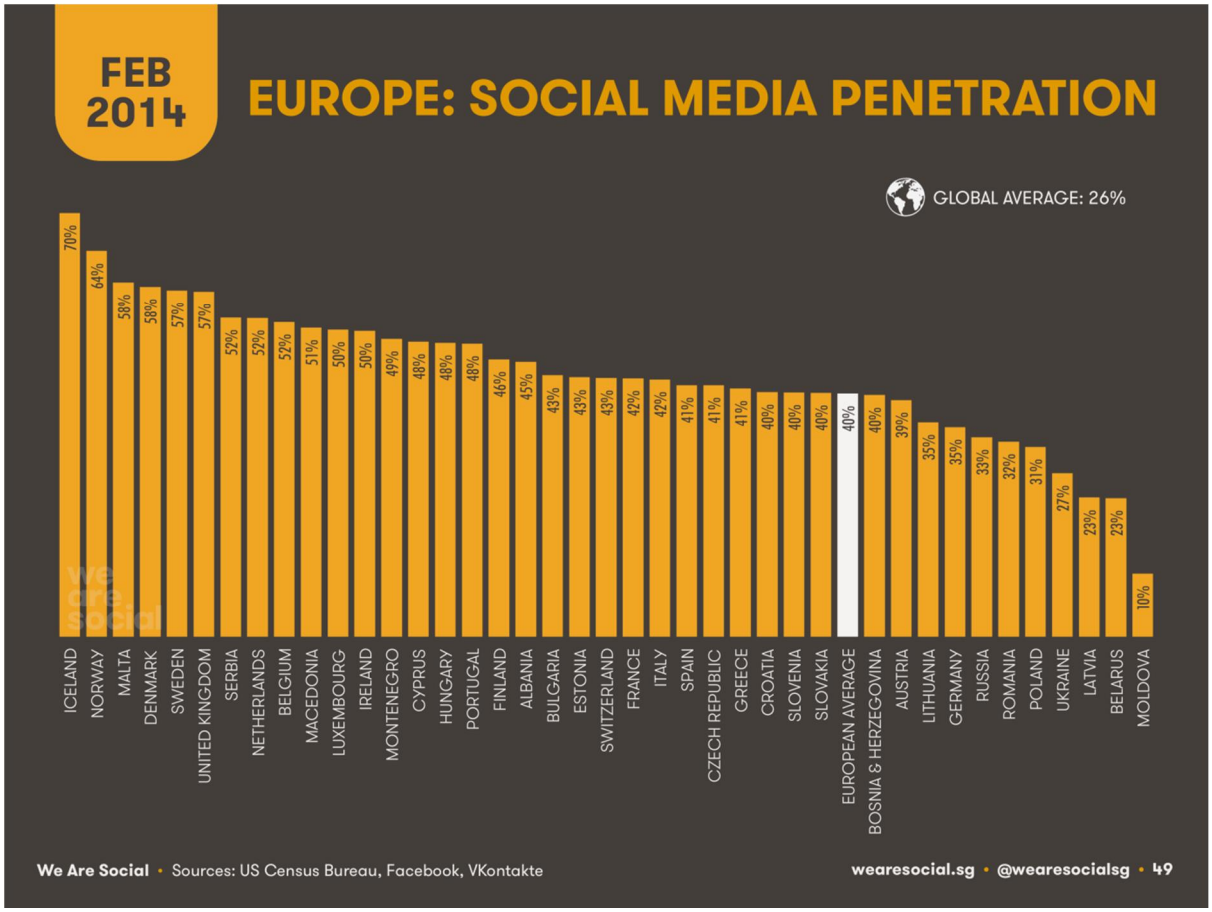


Figure: Social Media Use in European Countries

The European share of social media is over a quarter of the world traffic and to give some context to this level of impact we provide figures below for each of the focal countries on levels of household Internet access and averages on weekly or daily use of the Internet in the countries (figures are from 2013 and 2012 respectively).

Slovakia

- 75% of households have access to Internet[162]
- 80% of population use Internet weekly[163]

Germany

- 88% of households have access to Internet[164]
- 84% of population use Internet weekly[165]

[161] http://wearesocial.net/blog/2014/02/social-digital-mobile-europe-2014/
[162] For detailed account and trends see: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-12-050/EN/KS-SF-12-050-EN.PDF
[163] www.itu.int/en/ITU-D/.../Individuals_Internet_2000-2012.xls
[164] http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134
[165] www.itu.int/en/ITU-D/.../Individuals_Internet_2000-2012.xls

Italy

- 69% of households have access to Internet[166]
- 58% of population use Internet weekly[167]

Austria

- 81% of households have access to Internet[168]
- 81% of population use Internet weekly[169]

UK

- 88% of households have access to Internet[170]
- 87% of population use Internet weekly[171]

In drawing on the use of the Internet in Europe and in our 5 focal countries we highlight four main hypotheses that frame this chapter and we also seek to challenge understandings the impact of the Internet and social media use. We concentrate on:

- How and why do citizens use online technological innovations?
- How does an innovation such as social media affect understandings (attitudes) and the actions (behaviours) of citizens?
- Is there a dilemma between online and offline attitudes and behaviours?
- Is there a dilemma between privacy and sociality?

The chapter follows a structure of firstly discussing the impact of online technologies (section 4.1), for instance, online banking or email and how to some degree it has revolutionized the worlds we live in. Shopping, as another example, is now an altogether different proposition to what it was as recently as 15 years ago, the Internet for most is one of our first ports of call particularly when we want to secure competitive prices or research a potential purchase. The chapter relies on the inputs of our empirical research and it allows the voices of our interviewees to tell their story. In each section we concentrate on a central story, which is used to highlight the dilemma we pose in that section. The dilemmas focus on some of the trade-offs, difficulties, tensions or new socialites that, as we have found, are emerging in how citizens talk about Internet use (section 4.2). We also consider lives offline and the ever-increasing influences of the Internet and mobile technologies into issues of privacy and sociality evident in Europe today or during the summer of 2013, when the interviews were recorded (section 4.3). Finally we conclude by offer some thoughts and just how these aspects are actualised in Europe.

The chapter proceeds by looking at practices of using social media and concentrates on activities engaged in by citizens. These activities centre the on issue of *managing* ï where citizens actively maintain and care for their online profiles, identities and relationships. This focus is on the selective processes, for example, choosing online friends. The second focus is *using* and how the Internet and social media are engaged in by citizens, whether they are for

[166] http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134
[167] www.itu.int/en/ITU-D/.../Individuals_Internet_2000-2012.xls
[168] http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134
[169] www.itu.int/en/ITU-D/.../Individuals_Internet_2000-2012.xls
[170] http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134
[171] www.itu.int/en/ITU-D/.../Individuals_Internet_2000-2012.xls

example ópassiveô users ï who use the internet as a source of information ï or óactiveô users ï who blog, comment or post information online. The emphasis here is the act of doing and how things are initiated online and more explicitly how citizens live online. This focus will also link into some of the online lives and influences that now extend into offline behaviours and everyday life. The third focus is *upholding* and this refers to some of the legal parameters set in place to ensure the protection of citizensô rights when online, such as data protection rights. It also, however, looks to the online etiquettes that govern or certainly demand how social interactions are conducted online. Lastly we focus on *living* and socializing in a mediate world and argue there is evidence of new socialites emerging in how citizens live their lives online and offline. The impacts and commonalties citizens now share because of their lives online, as well as their lives offline, and the influences that chaperon such phenomena. We begin by discussing the role of technology and the Internet in our European contexts.

4.2 USING TECHNOLOGY AND THE INTERNET

As we have seen, a generous proportion of European Citizens are active online. Activities range from shopping, to dating, to using the Internet as a source of information. Other activities centre on promotional incentives where individuals and organisations advertise events or products. However, of huge significance to online life in Europe are the growing opportunities for social interaction online, with the rise of the web 2.0 the private use of the net seems to have become mainly about communication and socializing. Online tools such as emails, video conferencing or the ever-growing diversity of social media services have changed the landscape of how citizens talk to each other, as well as how business operates. No longer is the telephone or postal letter the main means of correspondence. What we refer to is not new, and email has certainly been widely used since the mid-1990s. Yet, it is the acceptance and normalization of these activities that have seized online sociality and to some degree offline sociality. For example, it is rare to now take a journey on any form of public transport without observing at least one fellow traveller using a smart phone, and one can presume, observing them checking emails or accessing the Internet. Equally these new technologies offer fantastic labour saving devices, for example, sharing online calendars.

What citizens do online has sparked much debate of late, sparked in no small way by the Snowden revelations. How information from social media is being used by governmental agencies, spammers or app developers is of growing concern to users.[172] For sociologists the narcissism inherent in the presentation of the online self and the formation and maintenance of online sociabilities has generated a litany of comment.[173] Arguments include the careful crafting of identities[174] or look to Milgramôs work on the inter-connectivity between people, and the 6 degrees of separation concept.[175] Many sociological arguments centre on the weakening of sociability as the social bonds and interactions of face-to-face behaviours and

[172] https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social
[173] Preece, Jenny. "Etiquette online: from nice to necessary." *Communications of the ACM* 47.4 (2004): 56-61.
[174] Rosen, Christine. "Virtual friendship and the new narcissism." *The New Atlantis: A Journal of Technology and Society* 17.2 (2007): 15-31.
[175] Milgram, Stanley. "The small world problem." *Psychology today* 2.1 (1967): 60-67.

networks are curtailed in favour of non-immediate or non-intimate online communications. Nevertheless, there is also a social strengthen in how citizens work, play, socialize and even engage in public or political debate and action online. Indeed, there is a cohesive community often evident in how citizens choose to participate online. As Barabási and Frangos suggest,[176] *ñThe world is shrinking because social links that would have died out a hundred years ago are kept alive and can be easily activated. The number of social links an individual can actively maintain has increased dramatically, bringing down the degrees of separation.ò*

For Barabási and Frangos the 6 degrees of separation, Milgram once proclaimed, can be reduced ï this concept suggests social relations are integrally interlinked and individuals are never more than 6 intermediaries apart. Barabási and Frangos argue that due to online relationships this separation has now lessened to 3. Indeed, the power apparent in social networks and media has been quickly harvested by political movements, as mentioned. The cause célèbre being the mobilization of voters in the elections of Obama in 2008 and 2012, when Facebook amongst other platforms was used in firstly identifying potential voters and then used to influence usersô voting. As Bond et. al.[177] excellent paper argues, influence is still spread through face-to-face social networks and the online political message sent by the Obama camp is at its most effective amongst those with strong offline ties. What citizens observe ógoodô friends doing online stimulates political thoughts and outlooks. Such micro-targeting, as Bennett[178] calls it, has culminated with election campaigns óin a boxô, where organisations now specialize in providing the capabilities to target specific audiences with the sole intention of influencing democratic practice. [179]

Sharing details online, be they political affiliations or allegiances, is de-rigour and something as causal as expressing a ólikeô on Facebook can indicate sensitive knowledge. For instance, likes have been used as indicators of preferences, sexual orientation, religious beliefs, illegal drug use and political allegiances.[180] This information is valuable in directing campaigns and indeed in providing strong indications as to demographic information, as well as, cultural and political leanings. Likes are a means of indicating your approval for comments or captions placed on Facebook. However, one problematic that comes to light in our interviews with citizens is issues of privacy and indeed, issues of prolific commentary. In relation to privacy, users do have the options to select and limit who views their posts, but are only too aware that organisations, such as Facebook or Google commonly use the entirety of their comments when analysing data. How people use social media can have detrimental effects as the frequency of posting can defy online norms. Posting too frequently and with too much detail can lead to viewers turn-off and restrict access to over-eager participants. In the following quote a participant gives some indication to the un-comfort they feel.

[176] Barabási, Albert-László, and Jennifer Frangos. *Linked: The New Science Of Networks Science Of Networks*. Basic Books, 2002. Page 39

[177] Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam DI Kramer, Cameron Marlow, Jaime E. Settle, and James H. Fowler. "A 61-million-person experiment in social influence and political mobilization." *Nature* 489, no. 7415 (2012): 295-298.

[178] Bennett, C. *Knowing how you vote before you do: micro-targeting, voter surveillance and democratic theory.* Session 9, SNN Conference, Barcelona 2014.

[179] Williams, Christine B., and Girish J. Gulati. "Social networks in political campaigns: Facebook and the 2006 midterm elections." *annual meeting of the American Political Science Association*. 2007.

[180] Kosinski, Michal, David Stillwell, and Thore Graepel. "Private traits and attributes are predictable from digital records of human behaviour." *Proceedings of the National Academy of Sciences* 110.15 (2013): 5802-5805.

Yes, the privacy settings. People who are not friends with me can just see the profile picture and thatôs it. é When I started using Facebook, in 2007 or something, nobody had that. It just developed in the last years. At the beginning, you could spy on everyone because there were no privacy settings (é) And I protect myself by not putting certain information on Facebook. Most of the time itôs just when I see something on the Internet then I share it. Or when I have an afternoon with my girlfriends and then we take a picture and post it. Itôs not too private information é not that I put every day how I am feeling and so é actually, I never do that (é) itôs also because I think it is not interesting that all my other friends are reading what I am doing. The people that are interested I phone them. And I think it is annoying the people that post something every day. Most of the time I also donôt post where I am at the moment é you could check in at places.ò

(Interview ID 536, 24 years, female, Austria)

The citizen is an experienced Facebook user and has some sense of pride in being at the forefront in maintaining her privacy. The participantôs guardedness is key here, despite her being a blogger and someone comfortable with life online. She is very selective in who has access to her online profile and highlights the fact that for her, if a person is important to her she would rather telephone than contact them through Facebook. We can presume these friends are also Facebook friends and to some degree this goes along with the findings of Bond et al that stronger relations remain offline[181] ï but what we do online or what we see close friends do online is important. However, most interesting in the comment is an awareness of self-selection where this experienced user is critical of overly exposing oneself. To blog or post too much is ónannoyingô. Equally, the participant limits the potential for others to locate her by not óchecking-inô. Yet, being online is a central means of communication for her, as she has practiced it for over 7 years and, judging by her age, many of her formative experiences may have revolved around online socialites. Nevertheless, for this participant at least there are a clear set of guidelines in how she performs online, care and attention are given to privacy and close friendships can be understood by those who she chooses to telephone. In the following section we extend our examination of how technologies encourage citizens to perform and concentrate on how online social media lives are manages by users.

4.3 SOCIAL MEDIA

Here we begin to dissect the attitudes and behaviours of citizens toward social media, and indeed the various issues of control and power that extol from citizens engagement with social media. Important are considerations of how information and the dissemination of that information have consequences in terms of how citizen data is being used by third parties. Much of the information placed on social media posts has value, as mentioned, that can be readily applied to political, financial or criminal motivations; however what citizens choose to place in their posts is also telling. What is posted often gives an indication of how citizens may be formulating the story or identity they wish to portray. Therefore section 6.2 has a

[181] Bond, 2012. Op. cit.

focus on the management of social media and how users control and manipulate how they use the platform and how they understand the impacts of this management. As we discover, participants in our research are aware of the implications of their posts and are aware that industries and governments may be watching their posts, but despite this, there appears to be a naivety or carefreeness attitude to in how some engage with social media, for others keeping a tight control is of concern.

Central to our observations and to the comments of participants are their deep and troubled appreciations of privacy and the making of online personas. Both aspects mutate and need management. Firstly in terms of privacy, as Albrechtslund[182] states, mediated publics are not private and there is a participatory surveillance to users proactive on social media. A privacy dynamic exists, in that users often feel they are in control of their information and what others can see. Through the functions available on sites limits are placed on accessibility for others, however as Boyd[183] warns what of the invisible audience, for whom privacy settings do not apply. Law enforcement agencies marketers and fraudsters, for example, can easily circumvent these limits. Equally through the networks users join or participate in, much can be gleaned or certainly inferred. More pressing still are the modifying qualities of social media platforms, where óimprovementsô to the functionality of sites, for example, establishing new links and commonalities with other users or creating new formats to present personal information such as photographs. In these instances when the changes are initiated, privacy settings are set to a default of open. For the privacy conscious user action is required. Andrejevic [184] speaks of ódigital enclosureô where every action generates information, and so nothing goes to waste. Indeed, social media offers much thought for surveillance studies because social media quantifies in very real ways the opinions and thought of individuals, because the interactions of users become measurable, traceable and visible and ultimately they are never forgotten.[185] Of interest to us is the notion here of collaboration in identity construction and in particular how the formatting of the sites moves users in certain directions, for example, using a photograph on a profile page and then mimicking the presentation of other users. As Castells[186] argues, the construction of identity is an organising principle and how users engage with particular audiences indicates the dynamics of those interactions. As mentioned earlier if a user is a member of a Facebook page for long distance running, it is safe to assume they have an active interest in this activity ï again all increasing the quantification of how users can be read.

Pressing in the following quote is how citizens are keeping control of their social media accounts. She begins by discussing the social media accounts she has,

[182] Albrechtslund, Anders. "Online social networking as participatory surveillance." *First Monday* 13.3 (2008).
[183] Boyd, Dannah,. ñSocial network sites: Public, private, or what?ò *The Knowledge Tree*, edition 13 (May), 2007a, at http://kt.flexiblelearning.net.au/tkt2007/?page_id=28.
[184] Andrejevic, Mark. *iSpy: Surveillance and power in the interactive era*. University of Kansas, 2009.
[185] Trottier, Daniel, and David Lyon. "Key features of social media surveillance." In, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.) Routledge. Routlege, New York. (2012): pp 89- 105
[186] Castells, Manuel. "The rise of the network society. Vol. 1 of The information age: Economy, society and culture." *Massachusetts and Oxford: Blackwell* (1996).

ñYes, I use FB, Twitter, Linkedin and YouTube. I have really tight privacy settings being aware that my data are lost anyway, namely that my privacy settings donôt protect me from Mr. Facebook who can use my data for aims I donôt even knowé . I donôt put my email and phone number on LinkedIn because LinkedIn is open. I put only my name and surname. é

I donôt use my name and surname in Twitter even though this does not protect me as Iôve been found by people I donôt necessarily want a direct connection with. I share opinions I am passionate about which I donôt consider ñsensitiveò. I avoid tweetting on politics because I am not so passionate about politics and I donôt have clear-cut political ideas. Data are lost anyway in Twitter. é

When I want to share something, Twitter is the last social network I use as the sharing practice is really fast and sometimes one does not think much about potential readers. é

In FB I use groups. When I share a video or a post sometimes I share it only within a certain group. In this sense, FB is easier as there are privacy settings. In Twitter there is no such thing and the problem is that Twitter is addictive but does not guarantee privacy at all. Black or white: the account is public or private. When I signed up on Twitter my account was private but then I went public as I was disconnected from the world and I "had" to go public. And I would do it again. Ideally one should have the opportunity to share in Twitter like in FB: you share ideas only with some people. Meets the criteriaò

(Interview ID 37, 27 years, female, Italy)

To the forefront of the participantsô comments are her provocations about privacy on social media. ó*Mr. Facebook*ô as she rightly indicates in one of the many faceless audiences that have access to her information. Interestingly she also refers to ó*sensitive*ô information and passionate opinions, which drive her posts. Avoiding topics, of course, may be linked to her lack of interest or knowledge and therefore she is reticent about commenting. All of which helps in the construction of her online identity as she registers her interests in the posts she does make. Nevertheless, there are clear demonstrations of power, trust and control in how the participant speaks of managing her account and the worries and concerns she has about her privacy and the security of her data. Indeed, note-worthy is the time-lapse of Twitter. Twitter for her is too instant and therefore has the greater potential of posting something that may be regretted at a later date.

Managing profiles by deleting and up-dating information allows for an editorial process in the construction of online presence. The audience and who they are dictate access to accounts and what they can and cannot view. ó*Mr Facebook*ô will always have the opportunity to view, however the participant does not want ó*too much*ô information online, because privacy is important. The participant has also considered erasing their profile, but to do so would have led to disconnection with family and friends. The fear of detachment is also of concern to the following participant,

> *ñI decided to boycott FB, but I did not want to have my profile erased, because I have these friends abroad and I want to stay in touch with them. I think it [FB] is addictive and people lose personal contact with eachéI think that people use Facebook because they want to share their privacy, be like an open book, what they do, when they do it, where he is. People post pictures with their friends; I think this is a loss of privacy.ò*
>
> (Interview ID 458, 37 years, male, Slovakia)

A compulsion or the necessity to stay online are a forceful influence and as the participant states they sought to boycott Facebook, yet they still wanted to use it for connecting with friends, which raises the issue if it was really a boycott. We want to finish this section, by suggesting that there is deep-seated compulsion within social media and one based on a fear of not-knowing or isolation. Indeed, many of the quotes we collected referred to social media as a source of information.

> *ñYou need to be part of certain things. If not, one doesnôt get to know/hear about anything anymore, for example Facebook. My nieces and also nephews é do a lot there, and I got to know all of that when I am on Facebook. Thank god, they donôt block me (hihi) so, I do get the information. Otherwise, I would find Facebook superfluous é On the other hand, I am a church guide. I frequently find things [on Facebook] that are quiet important for my work. There are old views [pictures] of our church and the like é on Facebook where people would not expect it. One can also connect with people, one can get to know people that I would not get to know otherwise because they are not in my [social] environment é I have an account on Twitteré I always read what my nephew does occupationally. That is also interesting, or what another nephew does é then there are the sites/networks for elderly, like senior.com, that I barely use.ò*
>
> (Interview ID 175, 63 years, female, Austria)

Using social media as a promotional tool, as some do, to highlight information is different to the management of the tool as an essential and it would seem addictive entity. Being online, being connected and posting can overpower the management of the tool. Even in instances where the compulsive nature of a participantôs use is acknowledged, concerns about privacy are raised and despite these concerns the tool is still used. This is not to dismiss the many advantages of social media which was touched upon in the introduction, but it does highlight the surveillance potential inherent in the activity and in the production of data. As social commentators caution, within social media, sociability and personal networks become very visible.[187] And while most of our participants were quick to acknowledge the prevalence and hazards of visibility, it would appear being connected is of greater importance.

[187] Trottier & Lyon 2012 op. cit.

4.3.1 Googleveillance

Alexander Neumann

In the last story an aunt was reading her nephews Twitter accounts to obtain information about them. This story highlights that social media sites are not only a source of information for users. These platforms also enable users to watch others members of these networks and simultaneously the watcher is becoming the watched as well. In other words many social media services enable the user to act as the surveillant whilst at the same time the surveillant user becomes surveilled by an anonymous group of other surveillants. Of course there is a third actor in this surveillance practice, the service providers. Google and Facebook are collecting and processing data about their users by means of dataveillance, data mining and profiling. While interviewing citizens about the integration of various communication technologies into their everyday lives, sooner or later many of them almost ñ*admitted*ò that they enjoy using services such as Google, Facebook, Twitter and the like to ñ*check on other*ò people they have just met or they want to meet in ñ*real life*ò soon. Surveillance studies scholar Fernando Bruno[188] describes this practice as participatory surveillance. Where, through such practices, users of Web 2.0 platforms constitute a participatory panopticon. The term participatory panopticon was coined by Cascio[189] and describes cyberspace, especially the Web 2.0 as a realm where a bottom-up version of the constantly watched society is developing. One can find a large variety of examples for participatory surveillance as explained by Bruno and Casico on sites like *crime maps* or *wikicrimes* where Internet users are collaboratively producing reports on criminal incidents in their neighbourhood. Separate from these practices, research in IRISS identified the fact that users are watching their peers or even complete strangers online through googleveillance. A good example of what is meant by the term googleveillance is provided by a story already quoted above.

> ***ñ****I posted something controversial when I was drunk, you know about it, you also read it. Not for the first time, but I had begun a new job recently and when I woke up, I really felt bad about it. My new boss even read it, made jokes about it and all. But on Sunday morning, it's like the whole world is on Facebook, I received comments from people I haven't seen in years and I thought, no, no more of that****ò***.
>
> (Interview ID 66, 31 years, female, Germany)

Borrowing from the famous *don't drink and drive* slogan for the ñ*Generation Facebook*ò the saying *don't drink and Facebook* has become a popular quotation that can be found on several social networks when someone obviously posted something under the influence of alcohol. In the narrative above, a young person from Germany regrets a Facebook comment she posted when she was drunk. People probably start to tell stories or make comments when they are drunk, which they often regret the following day. What is new about this story is the problem for the citizen as techno-social hybrid to actively provide for his/her privacy. Of course the controversial posting can be deleted the next morning when sobriety has returned, but in a world where everyone is on Facebook on Sunday morning and not sharing the gossip of last night's pub escapades on the church stairs, keeping-up privacy in the global village becomes a problem for the techno-social hybrid. There are two other interesting aspects in this story.

[188] See Bruno, Farnanda. ó Survaillance and participation on Web 2.0ô in Ä*Routledge Handbook of Surveillance Studies***ñ** Ball, K, D. Hagerty and D. Lyon (Eds.), Routledge New York, 2012.
[189] Casico, Jemais, *The rise of the participatory panopticon,* The World Changing, 4 May 2005.

Firstly, the linking of private and professional life on social networks: As the storytellerôs new boss is also part of her Facebook friends the storyteller comes to the conclusion, that in the future she will better consider what is to be shared with her Facebook friends. Second, the decoupling of time and space is obviously the biggest advantage of all Internet based communication. In this narrative the *virtual* friends of the storyteller, whom she hasnôt met or seen for years personally and who are now commenting on the embarrassing drunk Facebook posting seem to become very *real* the morning after. One could get the impression that googleveillance is a phenomenon experienced only by the younger generation, who are using social media platforms more frequently, where the distinction between real and virtual life begins to blur. However, this is not entirely the case as the next story from Austria highlights.

> *ĂBasically everyone who is my friend in real life is also my friend on Facebook, also my former colleagues or students. Especially many of my former students are my friends on Facebook,that is quite interesting. I can look what they are doing or I look what my grandchildren are doing or my son. I myself do nothing on Facebook. I also have an account on LinkedIn but I donôt use it. I wanted to share my experiences as a consultant for teachers on LinkedIn, but that was to stressful to me and you have to know that teachers are very bad clients (laughs).ò*
>
> (Interview 256, female, 77 years, Austria)

Interestingly social media platforms seem to be a vital source of information for family members to gather information about their relatives, although no one would ever consider this a surveillance practice: Neither the aunt reading her nephewsô accounts on Twitter or the grandmother in this story would say that they are watching their loved ones. Stories like the ones mentioned here represent a fundamental change in the relations of communication brought about through social media platforms. While checking on your relativesô status updates on Facebook is one thing, the borders between work and private life become increasingly blurred on these platforms. It is not surprisingly that the professional network LinkedIn launched its latest advertising campaign with the slogan ñFacebook for your private life and LinkedIn for your professional lifeò. As explained by the storyteller in the story above this slogan applies for her, as she tried to make use of LinkedIn as a platform to sell her services as a consultant to teachers. However, it is not so true anymore when Facebook information is used in a professional context as explained by the next storyteller form Italy.

> *ñOnce I should have employed a person in my husbandôs company, so beyond the CV I looked for information about him on Facebook. For instance I check the political opinions (I have many friends who are directors in big companies and they notice that the employees that are too much left-wing oriented usually are against the company owner) (é). I agree with this system of selecting the human resources, as on the Internet you can collect info about his behaviour, if he is a reliable person or the friends he has, (ñprofilingò his friends). (é) I check also if he writes on the Internet faked information about himself during the interview and I check if he says the truth on his Facebook profile. (é). Although I refuse to employ a person on the exclusive base of the Facebook information and I match them with the info collected through the interview, but I evaluate the person also on the base of practical motivation for the company (job experience, competence, etc.). At the end we did not employ this person but the motivation was beyond the Facebook info and the interview itself...ò*
>
> (Interview ID 206, 49 years, female, Italy)

This story is a good example how ICT paved the way for function creep and the changing power relations between employers and employees. In many of the interview passages that dealt with workplace related surveillance experiences (see chapter 5.2) the interviewees clearly supported the position that what they do after working hours is not their employerôs business. This is true for a time in which the borders between private and public or professional life where crisp but once you are friend with your Boss on a social media platform, then s/he is also your friend after 5pm. In the case of the Italian businesswoman the storyteller is explaining how she is using Facebook to look for information about potential employees. The profiling she is conducting is not based on Big Data or dataveillance, she simply checks the political opinions of the people that have been invited for a job interview and whether they tell her the truth during the job interview. Facebook was originally not designed to allow employers to get an impression about their next employee, but it enables employers to get a glimpse into the *private life* of their workers.

The last story in this sub-chapter on googleveillance is also related to Facebook activities and how a virtual profile can influence the life of citizens, although this story is more of a private nature than the one before. As the Italian job applicant in the previous story would have done well to use a fake user name for his Facebook profile to avoid awkward questions from his employer, the storyteller in the next story explains which difficulties he experienced precisely because of the use of a fake user name on Facebook.

> *A friend of mine always warned me to use a fake name. Actually this caused some trouble with my ex-girlfriend, as her friends have seen her engaging in a relationship on Facebook with an Indian sounding name they warned her to quit this relationship as this person, me, is only looking for a residence permit and not for true love. Iôve changed my fake profile name into my real one and also used a real picture of myself to avoid further troubles with her girlfriends.*
>
> (Interview ID 514, 37 years, male, Austria)

Using fake user names is a common strategy applied by many citizens interviewed in this study to protect their privacy on social media platforms. To some extent this strategy would qualify as a resilient practice as the surveilled user seeks to increase his/her privacy by doing so. In this story the fake user name strategy somehow backfired for the storyteller, as his fake name did not sound typically Austrian in the *eyes* of his girlfriendsô friends who checked on him on Facebook. The friends of his girlfriend came to the conclusion that, because of his foreign sounding name, he was a potential marriage imposter and that his girlfriend has to be warned about the upcoming tragedy. This led the storyteller to withdraw from his plans to increase his privacy on Facebook with a fake username and picture and he changed his user information and picture accordingly to avoid further troubles.

The googleveillance related stories should not be interpreted in the way that social media platforms enable citizens to surveil other users in the sense that they are collecting and processing data about the surveilled to influence their future behaviour. Googleveillance is a common strategy of gathering information about relatives, friends, employees or even people that users have never met before personally. The interpretation of this information is mostly based on gut instincts and is not a profiling of personal data to draw conclusions about a large population of surveilled individuals, but rather this phenomenon is part of the normalisation of surveillance in contemporary society.

4.3.2 Social Media and accepted practice

Keith Spiller

In this subsection we concentrate on some of the practices that accompany the use of social media. The first centres on issues of protection and legality, specifically issues of privacy and the data protection policies that govern social media. Then we consider some of the social etiquettes apparent when participating in social media and the accepted social interaction that direct social media use.

Legal protection

Max Schrems is a law student at the University of Vienna and over the past two years has challenged Facebookôs interpretation and application of EU data protection laws.[190] Schremsô complaint relates to the longevity that user data is retained by organizations and the practice of photo archiving data without user consent. Facebook insist they are working within the regulatory guidelines set by the EU Data Retention Laws and the Irish Data Protection Commissioner (the European headquarters of Facebook is in Dublin) is satisfied the organizationôs data protection practices are legal. The challenge made by Schrems and his group *Europe-v-Facebook* has taken the dispute to the Irish High Court; which on June 18th 2014 referred the case to the European Court of Justice.[191] This action draws attention to the types of data held by social media organizations, in particular how information is handled, stored and traded all of which raises pertinent data protection questions. And as Schrems suggests, this is not an issue limited to young users of social media ï young people do care about the privacy of their data.[192] Instead, this is a larger problem affecting all users. Much of the problematic surrounding social media data is a lack of clear policy and regulation.

Under the EU data protection framework users must consent to their data being used and collected and information can only be used in situations were consent has been given.[193] However, where this becomes deeply complicated is the multifarious means in which information is shared on social media platforms and when national security interventions take precedence over privacy.[194] While users are appeased with a sense of control[195] in how they can set their personal profiles, other areas are more difficult to manage; for example interpretations and analysis of *likes*. Current civil right law, data protection law and copyright law are unsuited to the demand placed on them by social media.[196] Important here is the context of the interaction and level of interaction, because consent, for example, is not

[190] http://www.nytimes.com/2012/12/05/technology/austrian-group-plans-court-challenge-to-facebooks-privacy-policies.html?_r=0

[191] http://www.independent.ie/irish-news/courts/europe-v-facebook-higher-court-to-decide-on-giving-data-to-spies-30367044.html

[192] Bonneau, Joseph, and Sören Preibusch. "The privacy jungle: On the market for data protection in social networks." *Economics of information security and privacy*. Springer US, 2010. 121-167.

[193] Danezis, George. "Inferring privacy policies for social networking services." In *Proceedings of the 2nd ACM workshop on Security and artificial intelligence*, pp. 5-10. ACM, 2009.

[194] See http://www.theguardian.com/world/2014/mar/27/google-youtube-ban-turkey-erdogan and http://www.nationaljournal.com/tech/the-nsa-is-using-facebook-to-hack-into-your-computer-20140312

[195] 26% of EU social network users feel they have total control of their data, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

[196] http://www.irishtimes.com/business/sectors/technology/citizens-need-to-ask-why-their-data-is-being-held-online-1.1801157

explicitly labelled to apply to policy that regulates social media. [197] More attention is needed on the detail on how the data is being used and by whom and in what situation ï for example, consent for *likes* to be gathered and analysed. In this regard a recent open letter by leading literary figures to the UN calls for, an International Bill of Digital Rights, they state,[198]

> ***ñ****WE DEMAND THE RIGHT for all people to determine, as democratic citizens, to what extent their personal data may be legally collected, stored and processed, and by whom; to obtain information on where their data is stored and how it is being used; to obtain the deletion of their data if it has been illegally collected and stored.****ò***

As they state, an explicit understanding of what is being consented and by whom needs development. One development that has taken place is the introduction of the óright to be forgottenô. The European Court of Justice ruled in May 2014 that user data must be deleted if requested.[199] This case centred on the removal of links to "out-dated, wrong or irrelevant" information; therefore if a citizen requests Google to remove links to out-of-date data, Google search results will then not display the information. The information does not disappear and could be found through other resources, for instance, newspaper archives; however Google are prevented from finding and presenting the information. The warning óSome results may have been removed under data protection law in Europeô appears on search results. This law only applies to European searches and is not evident in searches made elsewhere in the world.[200] Despite the impact of this development, privacy concerns still exist, especially with regard to data being used in a responsible manner.[201] This, no doubt, is complicated by the multitude of ways users provide and produce data to, for instance, social media sites. Finding an adequate framework to counter data protection concerns obviously needs direction.[202] Moreover, users are now increasingly aware of these discrepancies and are demanding adequate protection.

User etiquette

Participating in social media follows, as mentioned, certain parameters and rules. There are restrictions on how much a user can write on some sites, while in others there are set formats to be followed, for instance only writing on ówallsô. Interestingly, one of the successes of an early network site, MySpace, was due to a code gap in the page design, where users were able to personalize the background display of their profile page.[203] Most of the more recent network sites however have produced much more standardized page displays and functions. Recent academic work has looked to the homogenising effect of social media and networks. Farquhar[204] argues that much of the social capital of these networks is based on the interpretation of others and the formation of identities that are used to ensure entry to preferable groups. Getting into the óinô group encourages exaggerated performances that are

[197] idbid
[198] http://www.theguardian.com/world/2013/dec/10/international-bill-digital-rights-petition-text
[199] http://www.irishtimes.com/business/sectors/technology/citizens-need-to-ask-why-their-data-is-being-held-online-1.1801157
[200] See, http://www.theguardian.com/technology/2014/jun/26/google-removing-right-to-be-forgotten-links and http://www.bbc.co.uk/news/technology-27631001
[201] Business Life, 2014, op. cit.
[202]http://podcasts.ox.ac.uk/data-protection-and-social-networks, Brown, I., 2012.
[203] Boyd, 2007, op. cit
[204] Farquhar, Lee Keenan. "Identity negotiation on Facebook. com." Unpublished PhD Thesis University of Iowa.

designed to appeal and conform to the inferred preferences and approval of the online group. In this manner behaviours are tailored to the perceived interpretations of others.[205] In other instances conformity is driven by the desire for privacy, where for example children post conventional opinions due to an online parental gaze. As Brandtzæg et al suggest, many older social media users begin using social media in order to monitor the behaviour of their children. [206] Nevertheless, the benefits of social media include having an extended audience and having all your friends in one place. Expediency and efficiency are guaranteed as a single notification can alert all to engagements, events or attitudes. However with catering for large audiences comes difficult social dynamics, one such example is the tailoring of comments to appease or not offend ï or on occasion comments designed to offend and bully.[207] Managing audiences through social media is a lattice of complexity and getting beyond certain numbers of friends and viewers can stimulate irritation.[208] Equally, the sometimes competitive nature of collecting large numbers of online friends has little or no correlation with emotional closeness offline or how a person interacts face-to-face with another person.[209] Social media enlivens a social etiquette that at times is very different to the social clues and indicators that lubricate offline sociability. New forms of sociability are established and these can be evidenced in the comments made by our interview participants. In the following quote the participant speaks of her online friendships.

> ñ*At the beginning, I wanted everyone, now I select more, on the other hand I do not want to offend anyone. I would like to leave Facebook altogether, but it is not possible, I mean, just for school, who is not on the Facebook like he does not exist. You will find everything there and the access to information is faster than in real life."*
>
> (Interview ID 632, 25 years, female, Slovakia)

As the participant states her original goal was to include any person who wished to join her friendship list. In time, this caused a quandary once she learned to be more selective, rejecting a friendship request or even de-friending an existing friend, although this carries the risk of offense. It would appear such selections can have far-reaching consequences. How these maybe realised in offline life is unclear, but certainly they have an impact for this participant. In addition, and much like some of our earlier discussions, the conundrum of leaving Facebook is also aired. Again, the desire is to leave but the fear of social isolation or separation is too great. To ǿexistô one must be on Facebook! Indeed, this form of existence may also create a need to continually express oneself in order to ensure one is visible, verbose and prolific ï all of which confirms an online presence or when done too much an online irritation. As the following participant suggests,

---

[205] Lewis, Kevin, Marco Gonzalez, and Jason Kaufman. "Social selection and peer influence in an online social network." *Proceedings of the National Academy of Sciences* 109, no. 1 (2012): 68-72.

[206] Brandtzæg, Petter Bae, Marika Lüders, and Jan Håvard Skjetne. "Too many Facebook ñfriendsò? Content sharing and sociability versus the need for privacy in social network sites." *Intl. Journal of Humanï Computer Interaction* 26.11-12 (2010): 1006-1030.

[207] Lenhart, Amanda, et al. "Teens, Kindness and Cruelty on Social Network Sites: How American Teens Navigate the New World of" Digital Citizenship"." *Pew Internet & American Life Project* (2011).

[208] Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology, 73*, 741ï 752.

[209] Pollet, Thomas V., Sam GB Roberts, and Robin IM Dunbar. "Use of social network sites and instant messaging does not lead to increased offline social network size, or to emotionally closer relationships with offline network members." *Cyberpsychology, Behaviour, and Social Networking* 14, no. 4 (2011): 253-258.

ñBut with Facebook I started to have problems with people that shared a lot of information with me, but in real life we had nothing to talk about. I had too much information about people, but I was not willing to filter between different groups."

(Interview ID 578, 25 years, male, Slovakia)

Evident in this quote are some of the contradictions inherent to social media practices. There is a desire to post and present an image and identity, but in the offline life there can be a distance or unease felt in dealing with real time sociabilities. These difficulties persist in the following quote,

ñI am aware of the risks Facebook brings ï you can easily find out a lot about a person. Sometimes I use it to look for some people and information about them. For example if I like some girl, and I donôt even need to know her name or anything, and sometimes I am able to find her and get some information about her. For example, I liked a girl who worked in the same building where our firms is. So I was thinking about how can I find her? My boss actually mentioned, that she does go to the same gym as him [crossfit] so I went to the Facebook page of the gym and looked at some pictures they posted there. I found an interesting picture of a pregnant girl working out so I looked who liked it and I found her there. Then I looked at her profile, checked out some pictures but I didnôt like them very much. (laughter) So itôs enough that you know one little thing and you can find the person.ò

(Interview ID 781, 28 years, male, Slovakia)

Here the difficulty is to some degree reversed, the real person appears attractive to the participant, but when she is viewed online her appeal wanes. Highlighted in these quotes are some of the new social etiquettes and practices surfacing through the use of social media. Two notable trends emerge in our estimation; the first is the perception of risk that accompanies not being online. If you do not have a social media presence then the likelihood is that the user will miss out on particular activities. There is also risk apparent in the division between online and real time living, as the quotes suggest, making judgements or inferring knowledge about a person is dependent on what can be learned online as well as what can be seen offline. The second trend relates to new found forms of social distance, in particular knowing when to curtail certain activities, such as posting too frequently. As well as the invasion of online personal space, for instance delving deeply into profiles or learning to cope with ordinariness in real life meetings and interactions. These trends, it would appear, uphold how citizens use social media and the social guidelines they abide-by in their activities.

4.3.3 Social Media and the social: My life online

As we have explored in previous sections, social media is now a well established and recognised phenomenon, for example, in 2013 ćtweetingô was added to the Oxford English Language Dictionary. Indeed, the vernacular and the activities of social media are now commonly used by presidents, rock stars, teachers and nurses alike. Stimulated by social media an emergence of unique and diverse activities has occurred and with it some unusual contexts in which social media has made deep impacts, for example, in health contexts citizens have often found solace and support with regard to particular conditions and

diseases.[210] In other instances, social media has been used to find information or report on new and distant places to live, study and work.[211] These aspects, and others, of social media have unsurprisingly spawned much academic enquiry and chief amongst these has been considerations of the personalities of those who predominately use social media. Correa et al. draw on character traits of extroversion, neuroticism and openness in establishing who uses social media.[212] Personality they state has strong correlations with social media use, for example, extroversion is positively associated due to opportunities to display and perform. While the distancing effect of online interaction holds appeal to those seeking support for emotional in-stability, it can also discourage and intimidate due to the non-anonymity expected when using some aspects of social media. Whereas, especially for older users, social media offers those with a tendency for openness to new experiences an avenue to experiment and participate. In what follows we focus on how social media is used and how users embrace the medium and how issues of self-censorship prevail in their online activities. Social media is a way of expanding friendships and is an avenue for extroversion or openness, but our intention here is to also draw on some of the interesting uses of social media that have arisen in our interviews.

In exploring this theme we concentrate on privacy ódabourô or how citizens often work to protect their privacy. This we suggest is not passive and as comments made earlier suggest privacy carries with it a need for vigilance. One such example of this kind of labour is sensitive health data, for instance how to maintain the confidentiality of patient information while also encouraging potential health developments and benefits.[213] Indeed as we will go on to discuss below the sensitivity of data, particularly financial or health data are issues of deep concern for many of those we spoke to. We begin with an example of the care taken by a participant and the warnings given to her and her fellow students at school:

> ***ñ****I would never put my location on Facebook. I wouldn't put personal information, like my phone number or my address on either of them. My photos are on Facebook, but on Twitter, I don't think I'd put any actual information about myself; it's more like what you're doing with friends. I'm aware that anyone can access your Tweets and things. I know in assembly at my school, they said we can see everything you're Tweeting and we're going to put someone's Tweet on the board and everyone really panicked...Yes, they got them up and there were all of these ones about people going out and not having done any homework and they put them on the board. They bleeped out the names, but they were people from my year's Tweets.****ò***
>
> ***ñ****It's a shock because you don't think that people would go that far to access your information. ... I think the emphasis was on if you put things out there, people can see them and he said it took me minutes to find these. I think that was definitely a wake-*

[210] Greene, Jeremy A., et al. "Online social networking by patients with diabetes: a qualitative evaluation of communication with Facebook." *Journal of general internal medicine* 26.3 (2011): 287-292.
[211] Sin, Sei-Ching Joanna, and Kyung-Sun Kim. "International students' everyday life information seeking: The informational value of social networking sites." *Library & Information Science Research* 35.2 (2013): 107-116.
[212] Correa, Teresa, Amber Willard Hinsley, and Homero Gil De Zuniga. "Who interacts on the Web?: The intersection of usersô personality and social media use." *Computers in Human Behaviour* 26.2 (2010): 247-253.
[213] Sweeney, Latanya. "k-anonymity: A model for protecting privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05 (2002): 557-570.

up call for a lot of people.. He was an IT teacher, so he was doing something on Internet safetyò

(Interview ID 6, 18 years, female, UK)

Evident in this quote is the ease of access to information posted online and the fear felt by students when that information was discussed by an audience it was not intended for. The participant it appears was careful in limiting the information she put online, but even for her it was a óshockô and evidently increased her awareness of online safety. All of which duly affects the labour she applies to her online self.

The next quote relates to posting something when drunk, equally what could be applied here is putting something on line when one was younger and a number of years later it resurfaces ï all relevant to the óright to be forgottenô ruling. These instances can and often do have repercussions for reputations, employability or even incarceration. Recent examples in the UK include Twitter users being jailed for posts made and the UK first Youth Police and Crime Commissioner having to resign due to defamatory posts she made when younger and drunk.[214] Other examples include the jailing of one individual due to derogatory racial driven comments made on Twitter or the harassment of campaigner Caroline Criado-Perez via Twitter.[215] The following participant expands on her drunken experience,

ñI posted something controversial when I was drunk é . Not for the first time, but I had begun a new job recently and when I woke up, I really felt bad about it. My new boss even read it, made jokes about it and all. But on Sunday morning, it's like the whole world is on Facebook, I received comments from citizens I haven't seen in years and I thought, no, no more that.ò

(Interview ID 66, 31 years, female, Germany)

In this instance the mistake by the participant ended with her closing her Facebook account, mainly due, it would seem, to the fact it was not the first time she had posted when drunk to calamitous effect.

We finish the section with what we consider as an unusual use of social media and one that demonstrates the growing research and insight this tool can provide, but also the ethical and moral challenges it creates. This quote refers to an adoptive parent viewing the Facebook account of his childôs birth mother. The mother had her privacy settings open and therefore nothing unlawful took place. However of note is the fact that he was instructed by the adoptive agency not to place images of his child online as her birth family could search or locate the child. Therefore his privacy setting were highly maintained and valued. He comments,

ñYes, absolutely, and I have to be careful as an adoptive parent. One of the things we talked about with the social workers was the danger of putting stuff online that would make you traceable to the birth parents, who might want to find you. Obviously itôs

[214] See, http://www.bbc.co.uk/news/uk-wales-17515992
http://www.theguardian.com/uk/2013/apr/21/paris-brown-no-action-twitter-comments
[215] see, http://www.bbc.co.uk/news/uk-wales-17515992 and http://www.bbc.co.uk/news/uk-25641941

important that [childôs name] has complete security, in terms of where she is, so stuff you would normally post online, talking about your kids, and maybe putting pictures up, or whateveré Actually, I donôt put pictures of my kids up. I know a lot of citizens do, but I just took that decision from the start that we werenôt going to do that. With [child's name], Iôve had to be extra careful so, for example, on Facebook I donôt mention her by name, which doesnôt make a big difference, really, but itôs just a precaution, and Iôve told friends offline not to say anything, not to refer to the adoption on Facebook.

When we were adopting, Iôd check the Facebook page of the birth mother, so I was able to check her out that way. She probably put certain things on there that she shouldnôt have done, so that made me quite aware of the fact that other citizens can just go in and read it.ò

(Interview ID 59, 42 years, male, UK)

A unique dilemma is evidenced here and most telling is what appears to be the reinforcement of certain contradictions enlivened by social media. The dilemma centres on privacy; on the one hand there is a strong emphasis on the privacy of the child and on the participant as well as his friends and family, as they too have made a concerted effort to privacy vigilant. However, Facebook in this instance has also been used to explore the page of a person who the participant might not have come across in other circumstances. Equally a rigid rule seems to apply in how the participant posts on social media. It can be presumed difficulties may also arise if it was found that the birth-mother and her family and friends were to view the participants ópenô page. There may not be a contradiction here because both parties are free to set their privacy settings as they wish, however issues of privacy labour are more telling. How privacy is maintained and understood it would appear differs greatly. Social media provides an opportunity to search and view intimate details of users and while attempts have been made by sites such as Facebook to protect the privacy of citizens, the consequence of viewing pages can be acute. The contradiction in this example may be the one-sidedness of access, in that one party can view and make observations but the other party is excluded.

The nature of social media is primarily a social tool in which friendship can be expanded and information and communications exchanged. This as we have mentioned can appeal to certain personality traits. Nevertheless, things can go wrong with social media and most pressing here is when defamatory or embarrassing material is circulated and the adverse outcomes of the exposure. The control of this information is given some safeguard due to privacy labour, but even here controls are easily circumvented and indeed are easily lost ï particularly if an óacceptedô friend has open privacy. Working to maintain privacy and working to avoid the consequence of information that has been posted is important. Again, drawing on the European Court ruling, the erasure of information is being taken seriously and the tentative reassurances provided by privacy settings are being superseded by stronger regulations. Needless to say as with privacy settings, getting around these controls is not difficult, for instance removing a court conviction from a search engine will not remove it from court records or even from newspaper records. However, it does stress that privacy labour in terms of online material may prove in the future to be more robust. Social media is a popular tool with undoubted social qualities, however at times it also needs to be treated carefully, particularly when used ill-advisedly.

4.4 MY LIFE OFFLINE

Regina Berglez

In this chapter the manifold interconnections between the offline sphere and the online life will be analysed with special emphasis on those stories of social media usage that yielded órealô consequences in positive as well as in negative terms.

4.4.1 Positive aspects: being connected

The adoption of other/ entirely different personalities in any given óonline worldô didnôt play a role for the interviewees in our study. However, they were clearly distinguishing, and indeed highlighting, certain aspects of their online selves ï most often in a very direct line to their offline life and with regard to certain roles. Respondents stressed their awareness towards the roles they actively take at various occasions in various networks - as friends, fans, relatives, employees, professionals etc. *ñFacebook is a multi-audience identity production site. The control users have over the privacy settings of their accounts enables them to partition their Facebook pages into many ôbackô and ôfrontô regions (é) whereby staging different identity shows for different audience.ò*[216]

The interviewees were actively editing their roles accordingly, putting emphasis on those parts of their personalities that matter (to them) ï somewhat quite similar to the Goffmanian ófront stageô.[217] Modern forms of online interaction may vary greatly in scope compared to pre-Internet times, but the basic underlying mechanisms of human interaction donôt seem to have changed fundamentally yet. (Although the ways and forms of these interactions have, which is claimed already yielding consequences on the usersô perceptions and even brain activities.[218])

Also, the fact that there is a special óstageô (= forum, newsgroup, Facebook group, personal blog etc.) existing for an indefinite number of roles and (almost) every possible aspect of oneôs preferences, believe system/s, identity/identities available, makes it much easier to get connected. It is argued, that óthe webô is encouraging community, solidarity and even empathy, (that can all be build up and strengthened through social media). No penchant seems too strange, no need too special, no opinion, belief or ideology that unique, not to find comrades in the World Wide Web. A greater part of modern online individuals seek for almost everything first online - and most often successful. Information, commodities, necessities and satisfactions as well as porn; and, of utter importance, like-minded-people (for good or for bad). Positive aspects were often reported in a way that can be exemplified with the following quote:

> *ñFurthermore, Facebook gives me the opportunity to contact other people practicing the same sport I do,that live far from my city or even abroad, namely people that I would never have the occasion to meet them personally. Facebook gives me also the*

[216] Zhao, Shanyang, Sherri Gasmuck and Jason Martin, Identity construction on Facebook: Digital empowerment in anchored relationships, In: *Computers in Human Behavior*, Vol. 24, Is. 5, 2008, p. 1822.
(Zhao et al are referring to Goffman ibid.)

[217] Goffman; Erving, *The Presentation of Self in Everyday Life*. Harmondsworth: Penguin Books. 1987 (1959).

[218] Comp. American Psychological Association: http://www.apa.org/news/press/releases/2011/08/social-kids.aspx
Also: http://www.businessinsider.com/this-neuroscientist-worries-that-facebook-home-will-change-our-brains-2013-4
http://www.psychologytoday.com/blog/social-brain-social-mind/201310/is-facebook-ruining-our-brains

chance to meet people with whom I share the same interest for judo, as Iôm interested in exchange experience and opinions with them, besides I have the occasion to meet some of them personally.ò

(Interview ID 936, 20 years, male, Italy)

It was also emphasised that the being connected in social networks can and does ï without the need to actively stalk a person[219] ï reveal worthwhile information about this person and his or her offline life:

ñIf someone posts weird Facebook-stuff, you can tell a lot about his character. Also the e-mails he sends, the SMS and all those things, it affects. It is as if you would be late (for the job interview). It counts to the first impression. It rather bothers me that you have to include a picture in your application. This also affects and in other countries this isnôt even allowed anymore. You can influence what you post on Facebook. You can block everything, and on your profile picture you simply dontôt show yourself with a beer or something like that. They wonôt find me if I configure it this way.ò

(Interview ID 504, 21 years, female, Austria)

Also, Sofsky reminds us of the ñ*freedom to privacyò*, which he frames as *ñthe desire to remain undisturbedò*, seems for mankind most often of far less importance than the *ñdesire for approval, care, protection, or companionshipò*.[220]

4.4.2 The privacy online-offline misunderstanding

The following quote can be seen as allegorical for many stories in which respondents alluded to the blurriness of ôprivacyõ and furthermore for the described assumptions that privacy is still heavily connected to a ôrealõ space that is e.g. the family home:

I dontôt actually have a definition for privacy. What is private? I guess really my family and my home will probably be. Thatôs the inner boundary. You dontôt invade on my space or my family and if you do youôve got to give me a bloody good reason to do it and that probably will require a warrant so, which isé but I dontôt have a definition for it, isnôt that curious?

(Interview ID 469, 43 years, male, UK)

Privacy was most often regarded as somewhat indefinable (which is not surprising, given the fact that a consistent or distinct definition or a conceptual framework on privacy doesnôt even exist in the scientific community. The term privacy remains controversial and in flux and was even referred to as a conceptual jungle[221]).

Other interviewees expressed an inherent connection between their online and their offline lives. ôDoingõ social media wasnôt portrayed as something separate but rather expressed as the extension of various aspects of life into cyberspace. An extension indeed created with the help

[219] For googleveillance compare chapter ñ4.3.1 Googleveillanceò.
[220] Wolfgang Sofsky, *Das Prinzip Sicherheit*. Frankfurt am Main: S. Fischer Verlag, 2005, p. 148ff.
[221] Solove, Daniel J., *Understanding Privacy*, Harvard University Press 2008.

of fairly new tools, whether these were perceived as exiting, as normality, or ï in some cases ï fatiguing; but nevertheless tools. Tools that make it easier to stay in touch, stay informed, stay connected; despite the negative impact in terms of e.g. surveillance.

Following Goffman, we state that the role/s do matter in the presentation of self in a quite similar way online as they do offline. The next story is about a clear demarcation line between a personal self and a professional self ï which turns out not to be so clear after all. The interviewee is an early adopter of the Internet and spent two decades working in (subculture) media, using online-tools extensively ever since they became available. His statement illustrates in a somewhat emblematic manner the blurriness of the lines between oneôs roles online:

> ***ñ****I use Facebook quite a lot and for a long time for job reasons. Social media plays one of the most important roles in promoting our work. I divide very distinctively between the work purpose and the private use. I would never put something intimate on Facebook at all. I like to spread underground music, interesting articles etc.* ***ï*** *but private stuff stays out there. Once it is about private stuff I call the people or people have to call me, and true personal stuff is only for face-to-face meetings. Thatôs how I keep it ever since.****ò***
>
> (Interview ID 995, 44 years, male, Austria)

Asked, if such a division works out in everyday life, the storyteller went on as follows:

> ***ñ****Well, youôre right, I do see the point as well that a clear division between the general and the private is impossible. You can avoid posting personal stuff, but of course if you promote left-wing art your political opinion is obviously out there. But well, it is as it is. Whoever reads my printed articles can make this conclusion as well.****ò***
>
> (Interview ID 995, 44 years, male, Austria)

This exemplifies a really interesting point that seems to be a quite common misunderstanding, which is, that postings containing nothing óintimateô or ótrulyô private wouldnôt reveal anything about the private life of someone. As will be elaborated later in the conclusion of this chapter, not only Big Data already goes far beyond that.
Staying with this particular story, it can well be argued that much more information than ójustô his preferences in arts and music going along with his political opinions is open to everyone who would google him. However, in this case it has to be taken into account that the respondent is to some extent via his work already a public person although restricted to a special circle of fans that are interested in the particular topic.

Nevertheless, the respondent is putting lots of thought into which information is opened up ï respectively posted ï in terms of what is considered a óprivateô (i.e. ***ñ****my very own opinion****ò*** and what isnôt (i.e. ***ñ****I share articles I find interesting and worth spreading*ò) a common topic in the interviews.

Respondents not only highlighted this point, but also often act upon it in a certain way: Not posting óeverythingô everywhere, which is considered a strong protecting of their privacy. A

very crucial point here is, that what may well be termed a form of resilience is based in an offline perception of privacy. It could be seen as the somewhat pre-social media habit of dealing with the balance between openness and privacy transferred to social media, marking a demarcation line directly transferred from the offline everyday life.

> *ñWhat I post is exactly what I also would tell the persons who can read it, face-to-face, if I would meet those people. But I donât have everything available for everyone. I have lists, where I can say, áthis is something everyone can knowô but also lists where I say áthis is something I only want them to be able to read.ôBut the criteria are here and there the same, like in the daily life. There are some things, I wouldnât discuss with everyone.ò*
>
> (Interview ID 487, 32 years, male, Austria)

Unfortunately, the content of the given information is less the point than the functional relevance unfolding trough interconnections of data (sets). Baghai points out one of the crucial points in the wider context of how information creates power and vice versa[222] that ó[t]*he contention here is that privacy conflicts arise when an event in one social system becomes relevant, arguably without justification, to selection of communication in another system, e.g. when love affairs become thematic in evaluating professional competence; health conditions become relevant to securing a bank loan; or sexual orientations become relevant to employment. The public or private nature of communication is not determined by its content, i.e. whether it involves secrets, embarrassing or confidential information, or merely trivial daily transactions, rather, by its functional relevance to the social system in question. Thus, if the love affair involves oneôs subordinate, the health condition undermines oneôs ability to be party to a contract, and the employer happens to be the Catholic Church, the system reference and functional relevance of communication change and so do the legal contours of privacy.*ô[223]

4.4.3 Negative impact on the offline life

A negative perception of the overriding power of social media services is expressed as follows, pointing toward a separation of the individuals from each other based on the disintegrative sides of modern technologies:

> *ñIt is probably going to be loss of peopleôs ability to communicate with each other face to face and the addiction it causes as well. People donât realise it but when I wake up in the morning the first thing I do is check my phone for news and things, I just didnât do that when I was in the 1990s. (...) I think most people are addicted to it but they donât realise they are. If you look at any of your friends who have got smartphones and you often see them in the play parks, pick up the phone three minutes spare when the kidôs on the swingò.*
>
> (Interview ID 258, 37 years, male, UK)

[222] Foucault, Michel, The subject and power, *Critical Inquiry*, University of Chicago Press, 1982, pp. 777-795.
[223] Baghai, Katayoun, Privacy as a Human Right: A Sociological Theoryô, *Sociology* 46, nr. 5 (October 1), (2012): 951ï 965, p. 956.

Sometimes pressure to subscribe to social networks in order to stay informed was observed: This illustrates that the online sphere can take over in an unwanted way. In this case ï in order to arrange offline appointments ï rather harmless, as there are presumably other ways to arrange meetings ï so it might be rather a question of convenience than of necessity:

> *ñYou are just well connected, quick and instantly. So many people use it and I can find anybody there. So if you are not on, it may cause problems sometimes, in some contexts to arrange meetings to connect with other people.*
>
> (Interview ID 978, 33 years, female, Germany)

The next step is no longer having the choice in how ï or if ï to choose to seek and gain information online, but being forced into social networks, since the information gap created by staying away, is clearly not tolerable anymore:

> *ñWhen I started at the university I did not have an account, but because of my classmates I was basically forced to create one, because almost everything was solved through the Facebook and I did not want to be left behind. But I was very passive and just followed everything, without posting any content. After I started to work for NGO I was once again forced to re-evaluate my Facebook existence, as my job is about working with people, I started to use it also as a PR for NGO, started to post pictures, announcements, but everything is connected to my work, so there are no personal information there.ò*
>
> (Interview ID 594, 23 years, female, Slovakia)

Pressure, not even from self-chosen peer groups but rather through work-related circumstances where there is even less of a choice to resist is problematized as another negative side-effect of the all-encompassing presence of social media and the Internet, especially Facebook.

Far more serious is, for instance, hate-speech that directly extends into the offline life and can have serious consequences for the well-being of an individual. T the intensity and the dynamics of online shit storms and the like, show a momentum that could hardly be spawned or reached with respective offline activity (in the same timeframe and intensity).

> *ñI donât really have a problem of being in pictures from demonstrations, [gay] pride or when we went to parliament. I think its part of that and I am aware of the fact I will be in pictures. But on the other hand, taking into account the recent developments, it is scaring me a little bit. My friend, who is probably the best known lesbian activist gets lots of e-mails saying she will be beaten up or her girlfriend will be beaten up. So I donât know what I would do if that happened to me. She has to take a taxi everywhere all the time. But I donât really see any other way this can be done.ò*
>
> (Interview ID 770, 26 years, female, Slovakia)

That makes it very distinct that the comprehensive availability of e.g. photos of all sorts of events can create serious issues at all levels of everyday life for those that belong to, or

identify themselves as supporters of societal minorities that are subject to all sorts of discrimination ï or even (hate) crime.

Techno-securitization is slowly but steadily taking over the offline world and disadvantages for people who are objects of new control mechanism were mentioned as well:

> ñ*Well, not to the powers of the state, but in the football stadium, I have to identify myself via a bar code. This wasnôt the case a few years ago, when you could simply buy a ticket and get in. Now you have personalised [online] tickets, or at least I have with a year pass. And I was searched on entry. It takes much longer than before with those scanners.*ò
>
> (Interview ID 964, 57 years, male, Germany)

It should also not be forgotten, that óold-schoolô surveillance was already used for personalised advertising or for the collection of presumed or factual consumeristsô behaviours or preferences. The aim for data matching and the like is not an exclusive feature of the Internet era at all:

> *Back in the day, if I wanted to phone Germany, Iôd be put through an operator and if they had managed to get it sorted out, the operator would log where you were phoning to, then they could post you a leaflet being like, do you want to go on holiday to Germany? So this isnôt stuff that was never possible; itôs just made a lot easier now and so I suppose that sort of thing doesnôt worry me so much because itôs not something thatôsé I donôt feel that much more vulnerable. Itôs just it can be sometimes slightly more irritating because of how easy it is for people to bombard you with advertising and that kind of thing.(é) I donôt want Gmail reading my correspondence. I know itôs some robot thing, but I donôt want them reading myé I was more annoyed by that, when I felt that my correspondence, which I had thought of as private, was being, as I thought of it, read.*
>
> (Interview ID 141, 54 years, male, UK)

But, since several respondents stated, that there is *ñanyway no way back to pre-web timesò*, opinions like the following were also expressed, that represent óforward-approachesô of dealing with the novel challenges of social media:

> *ñIn some way, I donôt particularly like the idea ï itôs what I said before, really ï that there are all these nameless people knowing things about me, but on the other hand I just accept, well, thatôs modern life. The amount of information about me that must be out there: absolutely phenomenal.ò*
>
> (Interview ID 133, 69 years, female, UK)

Or it can even be taken further, as in the following statement that also characterizes a form of resilience:

ñNo, personally I am not afraid. To the contrary I am very open with my data. The more open you are the less they can make something unwanted out of it, twist it or else.ò

(Interview ID 970, 50 years, male, Germany)

4.5 CONCLUSION

Regina Berglez

The stories in this chapter unfolded around the various practices regarding social media in late modern times. The need and the willingness to use social media in order ï mainly but not exclusively ï to stay in contact with friends and beloved ones was expressed by most of the respondents. Although some interviewees described general concerns against the novel and suspicious services (of the Web 2.0) and depicted their reluctance against them, the vast majority portrayed the various advantages that social media services brought into their lives.

Most of the quotes in this chapter also included privacy issues; some stories involved various forms of resilience. Sometimes privacy concerns were expressed explicitly ï e.g. with regard to the Snowden revelations ï sometimes they were implicitly involved. Respondents characterized their use of social media mostly as an extension of their offline lives, either using a somewhat óoldô concept of privacy, or to some extent taking into account that privacy had recently undergone some changes that are as of yet hard to grasp.

Our theoretical approach to this dilemma on sociality and privacy assumed that the very need to use social media while at the same time making personal information available for a wider public would mark the core dilemma in this category, which can be confirmed.

There is clearly not *the* use of social media, but rather many different usages, usage patterns, shapes, and forms. It was ostentatious, that distinctions in social media practice were not only mentioned as side notes, but most often explicitly captured, focused on and even scrutinized. Highly specialized and customized forms of usages of the social web determined the greater picture given in the interviews. Social media (notably Facebook as the manifest and dominant example) does serve as a platform and a tool for sheer endless variations of self-expression ï and sometimes self-degradation ï information gathering, information spreading, up keeping as well as creation of relations and relationships, networking, and also controversy all the way to hate speech ï and, as a matter of fact, surveillance.

Indeed, a negative reading of óthe webô in a rather dystopian way ï either to a certain extent recalling Horkheimerôs and Adornoôs criticism of the mass media[224] and/or suspecting irrevocable separations of the individual based on disintegrative technologies ï was given by some respondents. The perception of a web-mediated world of allegedly highly individualised users that are taking selfies and spreading pictures of their daily meals all over the web is surely one side of the coin. Although excessive self-expression is undoubtedly a very real part

[224] Horkheimer, Max and Theodor Adorno, *Dialectic of Enlightenment: Philosophical Fragments*, Stanford University Press, 2002 (1944).

of the social web and was sometimes met with incomprehension by interviewees (especially those, that were not óheavy usersô or ódigital natives*ô* but rather interested ódigital immigrantsô), it wasnôt, after all, an assertive topic in the quotes. The dominant discourse was clearly a positive attitude toward the social web and all its possibilities.

In the previous chapter a perception of how to safeguard oneôs online-privacy was illustrated that might as well be termed a common misunderstanding: Respondents frequently seemed to rely on the (outmoded) concept, that posts, shares, likes or tweets which contained nothing órulyô intimate or private about themselves wouldnôt reveal much ï or even anything ï about them.
Not even needing to go as far as stating the common truism *ñthe private is politicalò* it can be argued that in times of Big Data this is just not the case anymore. Not only that political preference, personality scores, gender, sexual orientation, religion, or age, can be quite accurately concluded[225] by e.g. Facebook likes; but Jennifer Goldbeck even revealed how the liking of curled fries (on Facebook) has been linked to intelligence, since curled fries were *ñ(é) propagated through the network to a host of smart people, so that by the end, the action of liking the curly fries page is indicative of high intelligence, not because of the content, but because the actual action of liking reflects back the common attributes of other people who have done it.ò*[226]
Another example for how customized individual óonline-worldsô have become, is that of Eli Pariser, who demonstrated insistently how Google algorithms shape (respectively narrow) the results of an individual usersô search results based on his/her search history.[227]

A prototypical reaction that was described in the first dilemma on electronic commerce also played an important role in the reflections on the use of social media: the topic *ñWhat can I do?ò* Negative side effects ï to a great extent regarding privacy issues ï were noticed and explicitly expressed; but the advantages and the convenience factors do, however, override these concerns in daily practice; which is not to say that the respondents donôt take precautions. Nevertheless, precautions that go beyond the individual reflections and efforts to manage privacy i.e. paying special attention to what to post (or twitter) to which audience at a time, were rare. This could be exemplified with an extension or inversion of the humorous term PICNIC (person/problem in chair, not in computer), which is used by ICT-experts to describe the fact that a problem isnôt caused by the technology but rather by the user operating it. In a many of the stories cited in this chapter, the respondents clearly endeavour not to be the PICNICs regarding their privacy in the realm of social media. As it was argued in the previous section, the users make conscious and very distinctive decisions on what to reveal about themselves with a view to the specific platform used and the particular audience involved. Such provisions can clearly be grasped as strategies of resilience. Still, as was elaborated, Big Data is incrementally annulling these efforts.

---

[225] Kosinski, Michal, David Stillwell and Thore Graepel, "Private traits and attributes are predictable from digital records of human behaviour", *Proceedings of the National Academy of Sciences* 110.15, 2013: pp. 5802-5805.

[226] Goldbeck, Jennifer, The curly fry conundrum ï why Social Media ñlikesò say more than you might think. http://tedxesl.files.wordpress.com/2014/05/transcript-jennifer-golbeck1.pdf , Also: TED-Talk https://www.youtube.com/watch?v=hgWie9dnssU, both 2014.
[227] Pariser, Eli, *The filter bubble. What the internet is hiding from you,* Penguin, New York, 2012. Also: TED-Talk 2011: http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=en

However, forms of resilience that presuppose a rather complex technological knowledge as e.g. the use of encryption software; i.e. those actions that concern and shield privacy that operate on the level of technology (and not the person in the chair in front of the screen) are naturally not seen as a manageable option by the majority of ICT-lay citizens.

So it can well be stated, that*ñ[t]he concept of a (off-line) private sphere, defined in spatial terms of the private home (reaching back to the Greek notion of Oikos) is of no avail in the age of the Homo Electronicus and hence a redefinition of privacy is becoming inevitable. The boundaries between public and private domains ï and alongside with it the ósoldô concept of privacy ï seem blurred already.ò*[228]

Nevertheless and after all, the (social) web is a very powerful tool and maybe even the vernacular of late modern times. Quoting Kranzberg, one shouldnôt forget that technology is neither good nor bad nor neutral.[229] This will presumably stay this way whatever is to come, be it in terms of the web 2.0, the predicted web 3.0, the Internet of things; or in any other field of man-made technology. Perceiving óthe Internetô in a techno-centred way as either only the cure or only the disease would blatantly reduce the discourse.

At the end of the day the ways, forms and strategies of dealing with social media root back in not only social behaviour but also social perception. The online sphere and the offline sphere cannot be seen independently from each other, although some participants referred to their use of social media as if this took place in a separated sphere. But the actions and also the consequences of the actions described, made the complexity of the interconnections obvious.
ñThe alternative, everyday life perspective that is gaining prominence assumes that social behaviour is embedded in wider networks, and that these networks are sustained by various technologies and social practices. This view stresses that the Internet continues, maintains and extends relationships, that it is used to perform oneôs identity (é) and to spin webs of significance (é) in old as well as new ways. People will continue to meet in online environments, but these are not entirely separate from their physical lives and corporeal contexts. The socialization into online communities, the negotiation, reproduction and contestation of identities and the integration of computing technologies into everyday practices are some of the issues that cannot be understood as long as the online/offline dichotomy is sustained.ò[230]

Also going along with this, the pre-social media concept of privacy is no more ï now society has to find (better) ways of dealing with this fact. As Boyd states neatly: ñA*ny model of privacy that focuses on the control of information will fail. Even achieving true control is nearly impossible because control presumes many things that are often untenable.ò*[231]

---

[228] Berglez, Regina and Reinhard Kreissl, Report on security enhancing options that are not based on surveillance technologies, *SurPRISE Deliverable 3.3*, 2013., p.25. http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D-3.3-Report-on-security-enhancing-options-that-are-not-based-on-surveillance-technologies_v069.pdf

[229] Melvin Kranzberg, óTechnology and History: ñKranzbergôs Lawsòô, *Technology and Culture* 27, Nr. 3 (July 1986): pp. 544ï 560.

[230] Verschueren; Paul, From Virtual to everyday life, In: Jan Servaes & Nico Carpentier (ed.), *Towards a Sustainable Information Society*, Intellect, Bristol, UK Portland, OR, USA, 2005, p.179. Verschueren is also recurring to:
Goffman; Erving, *The Presentation of Self in Everyday Life*. Harmondsworth: Penguin Books. 1987 (1959). and Geertz, Clifford, *The Interpretation of Cultures*. New York: Basic Books, 1973.

[231] Boyd, Dana, Networked Privacy, *Surveillance & Society 10* (3/4), 2012, p. 349.

Big Data isnôt to be stopped ï but individualsô discrimination on the basis of this very data, is. This requires on the one hand a better public understanding of how social media and Big Data operate and what effects they can have; and on the other hand ambitious efforts are needed to create sound legal protection and a societal climate that goes against the usage of Big Data for the negative purposes of social sorting and discrimination.

5 4TH DILEMMA: PRIVACY AND TRUST ï FAIRNESS

5.1 INTRODUCTION: SECURITY AS A QUESTION OF TRUST

Reinhard Kreissl

One of the main resources providing for security in any social setting is trust. The perceived feeling of knowing what the significant others ï or in organisational settings ï the typified others are doing, sustains a climate of trust producing its mental corollary of perceived security. Proximity breeds trust. So does routine.[232] Trust is a core quality of stable social relations. As phenomenological sociology has demonstrated it can come in different versions, as personal trust and as generalized trust.[233] At the same time, trust performs a kind of limiting function. Trusting a person or a system limits the need for further enquires and scrutiny. Limiting further enquiries means to respect the private sphere of others. So privacy in social exchange is protected by trust. One could construe a simple trade-off here: *the higher the level of trust, the lower the need to collect confirmatory information about the other person*. The following chapter will play on this trade-off. It will consider a number of social settings where trust can be replaced by surveillance. These settings share a common feature that runs through this whole report: the increasing use of technology. Injecting technology into social processes has a number of different effects as we have seen in previous chapters. These changes can be analysed as creating different dilemmas regarding privacy. In the subsequent pages we will address the dilemma of trust and privacy. We also introduce a third mediating concept here: fairness. Fairness can be understood as an ethical concept defining standards of conduct that should be applied in a situation of unequal relations of power, as in the idea of a fair trial.[234] Hence, appeals to fairness come into play, when the misuse of power is addressed. In the context of the subsequent analysis, different social relations displaying clear power differentials are investigated: the sphere of the workplace, of the educational system and the relation between citizens and the state in a more general sense. In each case we have collected stories from our respondents dealing with technology-based surveillance, focusing on the relation of privacy and trust. Often the emerging dilemmas were seen through the ethical lens of fairness.

Surveillance, privacy and trust in workplace settings

While the relation between employer and employee is first and foremost of an economic nature, to be analysed in terms of wages and profits and capital and labour force, each workplace situation also entails an element of social interaction. The social relations in a workplace setting reproduce the economic relations of domination and submission, even if in many present-day work environments concepts like creativity, motivation, and personal satisfaction are invoked to describe the situation of the work force. In modern Western societies the model of the shop floor and the assembly line of industrial mass-production no longer provide the paradigmatic workplace scenario. The rise of the service economy, the integration of modern ICT in production processes, an increase in symbolic production and

[232] Garfinkel, Harold, A conception of and experiments with ātrustô as a condition of concerted stable actions. In Harvey, J.O. (ed.) *Motivation and social interaction.* Ronald, New York 1963.
[233] Schütz, Alfred, *The Phenonemology of the Social World.* Northwestern Uni Press, Evanston IL, 1967.
[234] The concept of fairness has been frequently invoked in assessing social relations in a political context, such as Trumanôs program of fair deal, an attempt to connect to the ñNew Dealò in the U.S. and later continued under the heading of ñGreat Societyò during the Johnson Administration.

design work, the international division of labour and the flexibility, volatility and fluidity of work, blurring the boundaries between private- and work life are just a few key words to account for the dramatic changes in the everyday situation of the working population.[235] What used to be a tangible and collective experience of exploitation in industrial capitalism has been transformed for a substantial segment of the work force into an abstract, often remotely controlled and intangible regime of self-motivated performance in a flexible work environment.

In the context of our analysis two of the most important changes are the emergence of a depersonalized relation between employers and employees, workers and supervisors and the availability of modern technologies, integrated into the work processes and creating a myriad of opportunities for surveillance. The supervisor, sitting at an alleviated desk, overseeing his team, has been replaced by the video camera, the electronic performance control, or the horizontal control regime of the ñquality circleò, at peer-to-peer level.[236]
Except for some niches in public service and areas with strong labour unions, control over performance, productivity, and output criteria have changed dramatically over the last decades. The balance of power between labour and capital in the era of ñheavy capitalismò, as Zygmunt Bauman called[237] it, has given way to a dominance of capital interests in the era of fluid or light capitalism, bringing the work force under a regime of what the late Pierre Bourdieu called *flexploitation*.[238] Surveillance practices are an important element of this regime. The situation here is somewhat similar to the domain of electronic consumerism analysed in the previous chapters, i.e. surveillance often emerges as a side effect of other management-related practices like auditing or controlling.[239] The introduction of new technologies not only changed production processes in an instrumental or material sense, but at the same time created new opportunities to monitor and surveill the work force. Issues of privacy and data protection emerged in this process in a similar way, as they became a topic of debate in society at large. While surveillance is seen as a problematic form of disciplining workers, there is also a dominant strain of discourse in organizational studies defending surveillance as a benevolent practice, increasing justice and identifying free riders and cheaters at work.[240]
To situate surveillance in the context of individual experience of social relations of work and labour one can draw on the concept of moral economy.[241] This concept developed in critical social and economic history studies, and focuses on the web of reciprocal obligations and expectations in economic relationships. It can be used to operationalize ideas like fairness and justice applied in the assessment of practices imposed by the apparent facticity of economic processes.

---

[235] See for a comprehensive overview of these changes Lash, Scott and John Urry, *Economies of signs and space*, Sage Publ. London 1994.
[236] see Delbridge, Rick and Turnbull, Peter,J., Human Resource Maximation: The Management of Labour under Just-In-Time Manufacturing Systems, in Blyton, Peter, Turnbull Peter, J. (eds.) *Reassessing Human resource Management*, Sage, London, 1992, p.56-73.
[237] Bauman, Zygmunt, *Liquid Modernity*, Cambridge Polity Press, 2000.
[238] Bourdieu, Pierre, *Acts of Resistance: Against the Tyranny of the Market*, The New Press, New York, 1998.
[239] See Power, Michael, *The Audit Society*, Oxford University Press, 1997.
[240] Sewell, Graham, and Barker, James, R., Coercion versus Care: Using irony to make sense of organizational surveillance. *Academy of Management Review*, Vol 31, No. 4, p.934-961, 2006.
[241] Thompson, Edward P., The Moral Economy of the English Crowd in the 18th Century. *Past & Present*, 50, pp. 76-136, 1971.

While contractual relations of labour law stipulate what each party of the labour contract is committed to do, it is assumed that both sides fulfil their obligations, since they more or less represent (morally) acceptable principles. This is a point Durkheim introduced in his Division of Labour.[242] Also it is assumed and mutually understood in this context, that formal regulations do not capture the daily routines of work. As Macnaughton-Smith pointed out in a seminal paper, in each organisational setting there are two codes in operation, and it is the informal and implicit ñsecond codeò that defines the relevant rules structuring routine performances.[243] Breaching this second, informal code can trigger formal sanctions, as laid down in the formal contract.

The spread of technology based surveillance practices in work place settings can be seen as a process eroding or transforming the operation of these informal rules. In the most general sense, the daily routines in any organisation require a horizontal and local understanding of how to do things properly among the involved actors. If this organisation has a hierarchical structure like most work environments, this mutual understanding also includes informal rules how to interact and behave in hierarchical situations. Such rules of conduct and performance emerge out of local practices, they remain implicit and are transmitted to novices through informal learning processes on the job and ï what is most important in this context ï they are of an analogical nature, allowing for contextual interpretation, adaptation and negotiation. Based on this second code the supervisor has to rely on the loyalty of his subordinates and the co-workers have to rely on the competence and cooperation of their colleagues, i.e. the ñsystemò works as long as all actors involved play according to the second code. The practical basis for such a regime is mutual trust. Trust seems to be a key variable for commitment and distributive justice in organisations.[244] Building up trust requires personal relations. It requires a continuous personal exchange among the members of an organisation, including informal shoptalk. Injecting ICT and surveillance technology in such an arrangement has a number of consequences. Person-to-person communication can be monitored, when a third party (i.e. supervisors, management) has access to personal exchanges e.g. through the intranet. Individual discretion with regard to the organisation of tasks and distribution of workload, flexibility of individual time and other formal criteria is reduced dramatically when all individual operations are documented and monitored remotely by an organisation through ICT.

Now while it may seem obvious from an external analytical perspective how the environment of the work place is transformed by new technologies and how new opportunities for surveillance emerge in this process for the management, it is far from clear how employees perceive this situation and how their daily routines are affected. Are they aware of these new surveillance regimes, can they verify their perceptions of being surveilled, do they know who is monitoring / surveilling them and how this is done? How do they react to the fact (the

[242] Durkheim, Emile, *The division of labour in society*, Simon and Schuster, New York, 1997 (1893).
[243] Macnaughton-Smith, Peter, The Second Code. Toward (or Away from) an Empiric Theory of Crime and Delinquency *Journal of Research in Crime and Delinquency* July 1968 vol. 5 no. 2 p. 189-197.
[244] Mukherjee, Kamal and Bhattacharya, Ranan, Exploring the Mediating Effect of Organizational Trust Between Organizational Justice Dimensions and Affective Commitment *Management and Labour Studies* February-May 2013 vol. 38 no. 1-2 p. 63-79.

feeling) of being surveilled in their performance? Do they invent any counterstrategies? [245]
Labour law has taken up the issue of workplace surveillance and unions are negotiating regulations regarding the use of surveillance technologies to monitor the workforce. National legislation beyond general data protection and privacy laws determines the limits of surveillance in workplace settings. But, as mentioned above, looking at formal codes of conduct or legal regulations governing the use of surveillance technology only scratches the surface of the problem of workplace surveillance. In their daily routines employees and managers do not use formal rules as a blueprint for action. Formal rules or for that matter any element of the formal organisation are invoked to retrospectively account for past events, making organisational action accountable.

We consider the effects of surveillance at the level of social relations at the workplace, trying to investigate and understand if and how surveillance replaces, undermines or erodes trust as a basic background resource, sustaining smooth and effective social processes in organisations. Hence from an analytical perspective we perceive of the stories referring to technology use in workplace environments as attempts to handle the dilemma of trust and privacy as a question of fairness.

Surveillance in the Educational system

The classroom has been considered alongside the factory and the panoptic prison as one of the paradigmatic sites for the emergence of modern disciplinary regimes, for control and surveillance. Educational settings like schools display a similar dual and contradictory structure like the workplace. On the one hand the main objective of the educational system traditionally has been the creation of docile bodies and minds, to paraphrase Foucault. On the other hand, every process of acquiring knowledge requires an active engagement of the learning subjects. So in any educational setting be it kindergarten, primary school or universities, the students are exposed to the contradictory regimes of bureaucratic order and autonomous individualism; they are supposed to meet the requirements of a standardized system of learning and at the same time are expected to develop into autonomous self-conscious or self-reflective individuals. What makes educational systems special is the layered order of power relations: teachers exercise power over their students but are themselves tied into the logic of the institution and governed by a regime of pedagogical rationality. And similar to the situation in the workplace, social relations in the educational system are undergoing significant changes triggered by the introduction of new technologies. Traditional forms of person-based surveillance and exercise of disciplinary power are supplemented, transformed, and moulded by new technologies. This has an effect on the regime of managing time, scholastic performance and general obedience to institutional regimes. What makes the educational institutions an interesting field to study individual reactions to surveillance is precisely their dual character producing a context of controlled autonomy, i.e. the main objective of education is the autonomous individual who at the same time is supposed to grow and develop under a regime of bureaucratically organized discipline. This creates the paradoxical constellation typical for surveillance societies: individuals are treated on the one hand as completely incompetent and on the other hand the default attitude

[245] see Marx, Gary, T., A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, Vol. 59, N0 2, 2003, p. 396-390.

of authorities towards their clients is suspicion. So while students are tied into a rigid regime of pre-defined learning modules leaving little room for individual, autonomous choice, they are under the constant surveillant gaze of the institution, as if they were habitual cheaters, trying to free ride the system.

Citizen, Surveillance and State

The relation between citizen and state is complex and has attracted many scholars. As Nietzsche in his Zarathustra famously put it: ñ*State is the name of the coldest of all monsters. Coldly it lies; and this lie slips from his mouth: ó***I***, the state, am the people.***ô**[246] Also Ernst Cassirer in his seminal book on The Myth of the State dissected the concept of the state as a symbolic form from Aristotle to contemporary times.[247] The history of political theory can be written in large parts as a history of the state and a good deal of social science literature invokes the notion of the state to analyse the reproduction of social order ï the old Hobbesian question.

For the lay citizen the state appears in many different forms and state power is encountered as representatives of public order ï policemen, public servants, and politicians. At the level of lay discourse the state is perceived as a collective actor endowed with a number of capacities and confronted with several tasks. States are supposed to provide public goods for their population. Security is one of these goods. And surveillance as a means to fight crime and terrorism and to provide for the security of the citizens is a dominant topic in the public debate about security. The capability of the state to ward off real or perceived security threats is perceived as a key indicator and source of political legitimacy. The gradual transformation of the modern welfare state into a security state (and security not referring to *social* security here) has been described from different perspectives. The growth of the technologically mediated bureaucratic web, restraining individual actions in exchange with public authorities can be investigated and analysed. But, again, what is of interest here is the perception of the individual citizen: how do citizens as clients of state bureaucracies perceive of and handle the fact of being under a constant regime of surveillance? How do they get around the rules, forcing them to behave in a pre-defined way to pre-defined standard situations?

5.2 CITIZENS AT THEIR WORKPLACE

Charles Leleux, Reinhard Kreissl

Surveillance in the workplace using information and communication technologies is a relatively new phenomenon, which is strongly linked to the changing structure of work.[248] Ball uses the example of call centres that *ó**has accelerated the diffusion of CBPM (Computer Based Performance Monitoring) in the United Kingdom**ô*[249], pointing out that *ó**organisations and surveillance go hand in hand.**ô*[250]

[246] Nietzsche, Friedrich; *Thus spoke Zarathustra (1.11: The New Idol)*, Cambridge University Press, 2008 (1883).
[247] Cassirer, Ernst, *The Myth of the State*, Yale University Press, New Haven, London, 2009 (1946).
[248] Hampson, Ian; Peter Ewer and Meg Smith, Post-Fordism and workplace change: towards a critical research agenda *Journal of Industrial Relations*, Sage Publications, 1994, 36, 2, pp. 231-257.
[249] Ball, Kirstie; David C. Wilson, Power, control and computer-based performance monitoring: repertoires, resistance and subjectivities, *Organization Studies*, Sage Publications, 2000, 21, 3, pp. 539-565.
[250] Ball, Kirstie, Workplace surveillance: an overview, *Labour History*, Taylor & Francis, 2010, 51, 1, pp. 87-106.

There has been a trend in recent times towards the creation of very large datasets of employee information using modern information and communication technologies.[251] The sharing[252] of data is becoming more commonplace, and is facilitated through the convenience of using adaptable and appropriate technologies. The rapidly changing nature of these modern technologies, coupled with changes in peopleôs working patterns and increasing use of portable technologies, such as smartphones, laptop computers and logging devices etc., has caused a blurring of the boundary lines between what constitutes ópersonalô and óbusinessô transactions and interactions.

This in turn has created conflicts and dilemmas for employers, employees and trade unions around the areas of reputational management, ethics, morals, trust, control and use of power.

Resultantly, this has necessitated the creation of new data protection and data processing legislation (or guides), and within the workplace itself, the drafting of new internal codes of conduct for employeesô and employersô responsibilities over the use of new technology, particularly where this involves Internet use, in an attempt to establish what is acceptable óuseô and what is not.

This has given rise to complex ethical tensions in the modern workplace.ô[253] In this chapter we will provide examples of the different types of surveillance practices and technologies, which are being deployed in the workplace. These technologies have become normalised,[254] and employees have accepted them, become resilient to them, resisted them or become resigned to their presence.[255] They moderate their behaviour in response to being monitored through the almost ubiquitous presence of surveillance practices and technologies.[256]

5.2.1 Being watched at the workplace ï CCTV

Being watched at the workplace can take on different forms ï from simple to sophisticated. Employees can be involved in such surveillance regimes in a number of ways: they can either be exposed to a crude and constant form of overt surveillance in their daily work routines, the simple approach. Or surveillance can take on complex forms, integrating the workers in an active way. Surveillance at the work place can remain simple by installing a CCTV camera on the shop floor or it can be intrusive by monitoring communication and workflows, covertly collecting data from technologies used by employees in their daily routine activities. Depending on the kind of work process there are different entry points for surveillance. Workers can be integrated in surveillance regimes, by convincing them that a constant and comprehensive monitoring of their daily work is in their own best interest (which of course is also the companyôs interest). The implementation of surveillance can be justified with the need to identify misbehaviour and rule breaking, what then amounts to a workplace specific version of the ideology of ñnothing to hide nothing to fearò.

---

[251] Higgs, Edward, *The Information State in England: The Central Collection of Information on Citizens since 1500*, Palgrave Macmillan, Basingstoke, England, 2004

[252] Bellamy, Christine; Perri 6, Charles Raab, Adam P. Warren and Catherine Heeney, Data sharing and personal privacy in contemporary public services: the social dynamics of ethical decision making, *Loughborough University Institutional Repository*, 2005.

[253] Sewell, Graham, and James R. Barker, Neither good, nor bad, but dangerous: Surveillance as an ethical paradox, *Ethics and Information Technology*, Springer, 2001, 3, 3, pp. 181-194.

[254] Ball, Kirstie, and David C. Wilson, Power, control and computer-based performance monitoring: repertoires, resistance and subjectivities, *Organization Studies*, Sage Publications, 2000, 21, 3, pp. 539-565.

[255] Ball, Kirstie, Workplace surveillance: an overview, *Labor History*, Taylor & Francis, 2010, 51, 1, pp. 87-106.

[256] Information on national regulatory regimes for workplace surveillance is provided in the Annex I on the country reports.

In any case the stories about workplace surveillance always refer to the relationship between employers and employees. Feelings of anger and irritation are sometimes expressed by employers due to concerns they have, e.g. theft, suspicion of theft, or reputational damage, and these feelings are expressed similarly by employees due to their discomfiture with being monitored, and the awareness that they are being watched and controlled.
Sometimes, the monitoring is carried out covertly, without the employeesô awareness, and it is common for monitoring of additional activities to take place over and above what was agreed originally due to the capability, opportunity and desire to do so. The asymmetrical distribution of power is clearly evident in some cases, e.g. ótop-downô from management towards employees. In some instances, monitoring is used as a means of compliance, by ensuring that employees conform to internal guidelines, the use of the Internet for example. Monitoring is also used as a means of rewarding good performance, and of punishing poor performance or perceived poor attitudes towards the employer personally or the company.

Sometimes workplace surveillance is overt, simple and ï due to the local conditions ï non negotiable. CCTV cameras are visible for the workers as in the first story below and the fact of these cameras being installed on the premises is justified under a rather crude pretext.

> *ñYes for example I've been working in Tyrol at a factory producing heating boilers. He (=the factory owner) had cameras all over the company premises to monitor the workers. Iôve been there twice during summer time. But officially he has these cameras to monitor the premises, to see if someone is entering the factory site who shouldnôt. As a matter of fact, he is controlling the workers. Everybody knows that. You donôt talk about that. Nobody has the courage to do something about it; itôs in a small village you know. Everyone knows everybody. Nobody has the courage to do something about it, he would go mad.ôô*
>
> (Interview ID 463, 34 years, male, Austria)

The storyteller here is in a powerless position, being watched in a kind of panoptical way from a boss who seems completely unwilling to negotiate with his workers. At the same time the technology applied, CCTV cameras, seems to be a simple add-on, a more or less primitive extension of the supervising gaze, extending the visual field ï at least in principle. From the workers perspective it is the mechanism of the panopticon: they know they can be constantly watched, but they do not know whether at any given moment their boss is really sitting in front of the video screen, following their movements.
An almost iconic relationship between the workforce and the factory owner is described in this story. For the workers it seems to be impossible to raise their voice against the fact that they are being monitored through video surveillance at their workplace. It seems impossible to overcome this intensified imbalance of power although there are labour unions in place and labour law is regulating the use of CCTV to monitor the work force. The factory owner appears as an irrational actor, who literally would ñgo madò should someone from the work force touch upon this issue. The story follows a simple logic: You canôt argue with a mad actor in a (working) relationship, you either quit your job or you surrender.

A more complex scenario ï technologically and strategically ï unfolds in the following story. Here an employer uses covert surveillance (CCTV and microphones) to control his workers.

The story is told by an Italian house painter detailing a case of over-surveillance at the workplace, through a misuse of CCTV systems and microphones for illegal surveillance of the employees. In contrast to the story from the Austrian part-time factory worker, the Italian house painterôs story shows some sort of an accomplice in the monitoring of employees with CCTV.

> *ñôI'm a house painter and I was doing restoration work in a company in the area where I live. As Iôm a friend of the electrician, he told me that the companyôs owner asked him to install many CCTVs and microphones all over the place, to control his employees. In fact, this company has been victim of some material theft where an employee was involved in this criminal activity and he was fired. Thereafter the owner decided to implement levels of control over his 50 employees. For this reason at the beginning he installed a CCTV system. Two years ago the situation degenerated, as the owner wanted to control also his employeesô conversations, therefore he asked the electrician to hide microphones for listening to the employeesô conversations everywhere: in the offices, bathrooms, corridors, as he wanted to spy on his employees and to know their opinion about him. The problem is that, if an employee expresses a bad opinion about his boss with other colleagues, the boss hears it through the microphones and usually transfers the person to a minor department, doing work that the majority of colleagues wouldnôt do. Nobody can denounce this situation, because they think that there is a colleague spying on themé this situation is still going on and the employees are still at the moment unaware of the spying activity of their boss, as the electrician keeps the secret about the hidden microphones, because the owner of this company gives him a lot of work and pays him well.ò*
>
> (Interview ID 106, 25 years, male, Italy)

As opposed to the first story, workers are given a good reason why they are being surveilled: CCTV cameras are installed to identify thieves among the work force. This involves the workers in a joint effort to identify wrongdoers. CCTV is introduced as a means to a mutually agreed end. But with the installation of hidden microphones the situation changes and the relevance of the concept of trust becomes obvious. Workers start to have second thoughts about the intensification of surveillance and they would like to exchange their views with colleagues. But since they do not know whether their conversation is being overheard or whether the person they talk to will report to the boss they refrain from doing so. This is a kind of micro-Stasi regime. Trust is eroding due to surveillance. The implicit rule of: trust thy neighbour (or in this case: thy workmate) no longer holds and this changes the social setting at the workplace. What can be observed here is a kind of chilling effect, similar to the reaction of citizens exposed to mass surveillance by police in public protest actions.

The next story increases the complexity of the surveillant assemblage. It represents a practical example of how an employer uses surveillance technologies, and a compliance officer, to monitor all aspects of employeesô online activities, and makes the employees aware of the code of conduct including giving reminders about what can and cannot be done online. The crucial point here is the introduction of a code of conduct in the first place: the employer introduces a code and then sets up a surveillance regime to make sure his employers comply with the code. From a logical point of view this story demonstrates the impact of new

technologies. Having access to the Internet creates new opportunities for employees (they can browse the Web, have internal chats, etc.). From the employerôs perspective this requires the implementation of a new code of conduct, regulating the proper use of ICT. Compliance is controlled using the very same technology the code of conduct is targeting.

> ñ*We have a guy who deals with welfare of the employees and I think that he has access to all of the information from our internal network chat, as well as all the websites we visit from the work computer and so on. I think that sometimes they [management] know things we did not say anywhere else but the chat and I am a bit cautious about what I write there. He makes sure that we adhere to the code of conduct. That includes the rules for what we can do and mustnôt do at the workplace, online. He is also in charge of security of our networks. Sometimes he helps other team leaders in the recruitment process of hiring new employees; he does some background checks on the applicants and so on. Information such as where you worked before, what you did there and whether you did not lie in your CV.*ò
>
> (Interview ID 726, 28 years, male, Slovakia)

Use is also made of the Internet and social media for background checks on prospective employees in this company. What this story nicely demonstrates is the powerful position of those employees who are competent users of ICT. The key figure, the ñ*guy who deals with welfare*ò is in the position to monitor all traffic on the intranet and also to help others in the recruitment process by screening the Web for personal information on applicantsô background. What can be observed here is the shift in hierarchies and the relative power positions of employees depending on how ñliterateò they are in using new technologies.

The final quote in this section is told from the position of the ñwatcherò. It is a story that comes from a team leader who, along with the manager, not only monitors employeesô project work via online tools, but uses the surveillance technologies to award premiums and annual salary rises. This story represents the mirror image of the employeesô perspective: while the ñwatchedò typically perceive of their being surveilled as negative, as a practice eroding trust and curtailing their freedom, the ñwatcherò interprets surveillance as a tool to distribute rewards and motivate his subordinates.

> ñ*I currently have 9 people under me and they have each to deal with some specific customers. When they deal with some problems, I can easily access what they are doing, for example communication with the customer via email, I can see their projects and their status and based on that I can ask them about their work. Me and the manager, we get reports of their work every day. Based on these reports, as well as information on how they communicate with the employees, whether they meet the deadlines, how much they work (they do), even after office hours, they get premiums and also a salary increase every year. And it is actually the same for me.*ò
>
> (Interview ID 729, 28 years, male, Slovakia)

The selected stories highlight how surveillance technologies are being perceived differently; how they are being used to reward good performance or to punish poor performance through the ways in which Computer Based Performance Monitoring (CBPM) is applied. What

clearly can be shown are the implicit dangers this technology brings, as it contains: *ódouble edged organizational öövalue orientationsôô ï there is the distributive justice of reward (material or otherwise) for effort and punishment for non-effort.ô*[257]

5.2.2 Being monitored at the workplace - timekeeping

Timekeeping systems have advanced over the years from the old fashioned time stamp clock to more sophisticated electronically mediated systems that collect, store and process data about employees. In this section some examples are provided of the benefits which are enjoyed by employees due to time recording, such as improved pay and more leave, but this has also caused jealousies with other employees who are not using the same recording system. It is clear that in some cases there is a level of acceptance of the technology and the regime being used, while in others it has created a culture of óclock-watchingô and resistance to the regime through adopting deviant behaviours by falsifying actual hours worked, and for example spending more time in the toilet than is necessary. In call centre environments a competitive element amongst workers has also been introduced through the use of surveillance technologies, involving monitoring of numbers of calls handled length of time taken etc. This has resulted in some employees adopting certain behaviours and forming negative attitudes towards other colleagues, to the detriment of social relationships.

The first story is from a call centre agent and demonstrates how continual surveillance in the workplace and focus on targets created an unsupportive environment and unhealthy competition amongst different teams and team members, resulting in deterioration in the value of human relationships and lack of care for a vulnerable member of staff. This story demonstrates quite well how the conformity of having to work in a call centre amidst the technologies which are used for monitoring of performance, sometimes does not sit very comfortably with more fundamental human values which one might expect when working with other members of a team:

> *ööIt created pressure in the organisation and got in the way of doing the job. You were pressured to work quickly which caused problems with teamwork targets and often created competition amongst groups and colleagues. I remember a woman in her 50ôs whose marriage broke down ï people did not like her because she was slower. Surveillance tools encourage that culture.ôô*
>
> (Interview ID 282, 24 years, male, UK)

What can be demonstrated here is the inherent contradiction of using teamwork models (such as e.g. quality circles) to increase the performance of groups. Under the specific conditions of tasks performed in a call centre, surveillance of workersô time is relatively easy and hence it is easy to compare differences in individual performance. ñBeing slowerò is collectively conceived as deviant or uncooperative behaviour. The effect is exclusion at the horizontal level. The underperforming individual receives negative feedback from her co-workers. The managementôs task to reprimand underperformers is thus taken over by colleagues. But in

[257] Ball, Kirstie, Categorizing the workers, in David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination,* Routledge, 2002, pp. 201-224.

order to identify a co-worker as being slower standards have to be implemented and a technical means to measure performance has to be established. While in a work setting of industrial production, such as e.g. an assembly line, temporal rhythms are defined simply by the machines, in an environment like a call centre individualized surveillance of each workerôs output has to be implemented since each individual performs in isolation as opposed to the assembly line, where the output of worker A provides the input for worker B and thus speed is the same for all. While call centres stand for an extreme, highly surveilled and highly exploitative environment, there are settings where employees can develop counter strategies to deal with the regime of time control. The second story draws attention to the fact that surveillance technologies can have a negative impact on employeesô attitude while at the same time not increasing individual performance or overall work productivity.

> *ôôYes, we had time registration. I remember lots of people standing round the attendance clock and wait for "one minute more, one minute more". Let's say: Those who have ever been lazy, they fought for every minute. Some did forget to check in, they didn't care because the work had to be done in no matter which time. It was my job to transfer the surplus of hours or the missing hours at the end of the month. But you saw it every time: Those who didn't like to work, they were the óminutes huntersôôô*
>
> (Interview ID 313, 55 years, female, Germany)

The final ótimekeepingô story conveys a similar message: employees trying to beat the time tracking system by adopting deviant behaviours, such as staying longer than required in the toilet. But there is a second important message encountered in many of the stories about workplace surveillance: the workplace setting is not perceived as a place structured by conflict and contradiction between capital and labour but as a social setting where mutual interests should be pursued to achieve a collective benefit ï in this case: higher profits to be shared with the employees. Time keeping is a strategy to make individual performance measurable and more or less transparent. Introducing the narrative of mutual interest (based on performance measures) provides at least a partial justification for the establishment of surveillance systems, which then are supposed to single out underperformers, cheaters and free riders. The underlying motive here seems to be a variation of the general theme of trust vs. surveillance: assuming that workers are willing and motivated there is no point in establishing a surveillance regime; but if it is assumed there are some who are not and who cannot be trusted, then surveillance may be justified.

> *ôôPersonally I believe that 70 to 80 per cent of all workers are recording their time correctly. 20 to 30 per cent are cheating. That is how it is. And if he is not cheating on the time tracking system he will stay for 15min longer on the toilet. I believe, that the motivation and the understanding of good and willing employees is key, of course money plays an important role and you have to explain to your employees why you are using a time recording system. But if we make a profit then it is also a profit for the employee. BMW and the other big companies are working like that. If we make profit we share it with the workers. If I would own a company I would do the same. Iôm a big supporter of this method.ôô*
>
> (Interview ID 343, 67 years, male, Austria)

The role of labour unions

An interesting position is taken by labour unions. They are supposed to represent the interests of their members and on the other hand to cooperate with the employers. They cannot ignore the caring side of surveillance, such as e.g. health and safety aspects, but have to consider any detrimental effects on privacy and autonomy. In the UK for example, trade unions will often go against their membersô wishes and support the introduction of workplace surveillance technologies where they feel that this will help with the health and safety of their members (employees), such as the introduction of body-worn CCTV for traffic wardens.[258]

A senior trade union official summarises the extent of surveillance technologies and practices used in his workplace (involving approximately 14,000 employees) in the quote below.

> *óóMonitoring of activities, timekeeping, monitoring of email usage, telephone records, Internet use, employers access to and use of medical information. All of these. Telephone records information is quite sophisticated: length of calls, ring time. Problems with employees accessing confidential records from major databases, and inappropriate use of email system to exchange jokes, cartoons or 3rd partyôs name/personal information. Also, growing use of social media to complain about employer/colleagues.ôô*
>
> (Interview ID 148, 53 years, male, UK)

The situation described here invites the following questions: is there sufficient justification for undertaking this level of surveillance; is this a good example of the employer exerting absolute control over the employees, or might the surveillance be more surreptitious and the employees are not really aware that it is happening, and finally, do health and safety concerns win over privacy and employment rights? It is hard for representatives from labour unions to come up with good answers to these questions, satisfying both sides ï capital and labour.

When it comes to negotiation of workplace surveillance at the level of collective bargaining procedures it is typically the worst-case scenario reasoning of security threats that is successfully introduced to justify the implementation of surveillance technologies. Protecting members of staff from assaults, threats and hazards is a catchall rhetorical figure and privacy concerns have to stand back when life and limb of workers are presumably at stake. The following story from a union representative who was involved in national level discussions around the introduction of CCTV in his industry shows how this logic operates. What is strikingly evident from this story is that the grounds for introducing CCTV were based on assaults on staff, however, CCTV was then used as a reason for introducing cost savings, such as closure of branches and stations, in effect creating a situation where vulnerable people travelling alone felt unsafe. CCTV was also used to assist in disciplinary investigations where the availability of CCTV footage was used not just in the case being investigated, but was used retrospectively too, particularly by junior managers wanting to be seen to be tough on employees. Clearly, trust between trade unions/employees and management has broken down

[258] Traffic wardens in the UK enforce parking restrictions through on the spot fines, and are seen by many members of the public as instruments of local authorities to generate additional income. They have been the subject of frequent verbal abuse and occasional physical assaults. It is known that some local authorities impose a ótargetô number of fines to be issued by each warden each day, e.g. five or six. The introduction of body-worn CCTV was introduced as a means of protecting these employees, but management have used the CCTV data for other purposes, such as investigating complaints.

in this situation, and the CCTV technology is being used to control employees. Additionally, it appears as though the closure of branches (due to the availability of CCTV) has been based on economic grounds and perhaps the unseen costs of increased fears of passengers who no longer have the protection of employees when travelling, but have to rely on the CCTV technology instead were not factored in:

> *óI was involved in the collective bargaining discussions around the introduction of CCTV in my industry, the argument for which was the number of assaults on staff and yobs spitting on staff. We worked in partnership with the police, and swab kits were introduced to help catch the yobs that were spitting. The installation of CCTV was to help identify muggers and assailants, and we welcomed its introduction as a trade union. But it was also used as a cost-cutting exercise by management making it easier to close branches and stations through conducting cost benefit analysis reviews, and saying that CCTV and helplines and phone lines for the public would be sufficient, but this was wrong as they did not reassure vulnerable women travelling alone. Some junior managers get promotion and want to make a name for themselves ï they use the tapes if an incident occurs and look to see what the staff were doing prior to the incident and then to start a disciplinary ï itôs outrageous!ò*
>
> (Interview ID 167, 66 years, male, UK)

5.2.3 Being controlled at the workplace - tracking technologies

So far we have presented various accounts of the types of surveillance technologies being deployed in the workplace. As could be seen in the stories presented above, behaviours are being moderated in many different ways by these technologies, and communication can be similarly restricted, thus affecting interpersonal relationships. In some cases surveillance technologies in the workplace have become normalised in terms of how people conduct their working lives. Management have the opportunity to use the technologies available to them for purposes other than those intended originally, sometimes in the context of victimising employees, although examples are also provided where the technologies have been used to help in the health and safety or welfare of employees. We started with simple CCTV schemes and moved on to more elaborate assemblages displaying more complex social effects. We will now turn to an even more intrusive form of workplace surveillance ï tracking technologies.

The next story demonstrates the precise level of control over employees, which can be achieved by installing a tracking device in their works vehicle, and by ensuring employees also use hand held tracking devices. Three main points are apparent: first, there are benefits to the employer through better productivity and easier programming of work; second, there are clear health and safety benefits to the employees if their vehicle breaks down, in that management or the employees can summon help to a precise location, and third, the surveillance technologies are being used in fact finding/disciplinary cases, which is a deviation from the original purposes for the introduction of these technologies:

> *ôôLocator, which is a vehicle tracking system put into the entire vehicle fleet. It caused big issues at the start, such as human rights. It was sold to us (i.e. the ócaseô was made) on the basis of reducing the insurance bill, and with vans not being used as much outside*

work, then they (management) could programme work better. Also, hand held devices (are used), which means that the majority of staff can work from home, reducing fuel and being more productive ï they reduce travel time and they can be a good thing ï we had a young chap (man) who was not answering because he had gone into a diabetic coma, and in the winter (poor driving conditions for example) management can monitor people getting home safely. One bad winter we had 4 managers working through the night contacting families letting them know where their loved one was. They (hand held devices) can be used for ófact findingô investigations, where employees are going home early or not arriving for work, or where the public are complaining ï Locator gives the number of the van and the registration. We have CCTV in the yards (industrial workplaces); Internet and telephone usage monitoring, and monitoring of Facebook.ôô

(Interview ID 159, 65 years, male, UK)

This is an interesting narrative since it emphasises all the good things that surveillance makes possible, saving money and employees lives, providing solace to the families of workers who got stuck in bad weather. The problem of workers being in an emergency situation probably is overstated and provides a justification for the introduction of highly intrusive surveillance technologies serving economic ends defined by the company.

The final quote in this section represents an attitude often found in discussions about workplace surveillance. Surveillance technologies have become normalised and the individual exposed to an ever denser and more intrusive surveillance regime surrenders to the fact of being constantly forced to demonstrate who he is and that he is legitimately doing the things he does in the workplace:

ôôI have experienced many surveillance technologies. Iôve been working there [oil refinery] for 30 years and the use of these technologies have increased. I donôt pay attention to them anymore. At the beginning I was annoyed but now I am used to them. I donôt talk about this topic with my colleagues. Nobody seems to care. There are lots of surveillance cameras and we have badges either to access to any areas or to provide access to a computer. I canôt log in without my badge. Everything is monitored but itôs understandable. It's for security reasons.ôô

(Interview ID 577, 50 years, male, Italy)

5.2.4 Feeling of being spied on at the workplace ï Facebook, Google and the like

There are many examples provided in the interviews of the widespread use by employers of googleveillance and other forms of social media to check both on the activities of candidates for positions, and of existing employees. Some elements of social sorting by employers are evident from these practices. Resistant and deviant behaviour also takes place by some employees to the practice of monitoring their online activities. The use of googleveillance and other social media for checking on the private activities of employees or prospective employees brings the issue around the ópublicô and the óprivateô firmly into the debate. Wigorts Yngvesson describes the *óprivate and public sphereô* in the context of human relationships, which are fluid and do not have defined boundaries: *ôThey have boundaries*

which vary according to circumstances.ö[259] In this context, workplace surveillance technologies are no respecters of privacy or private activities due to the universality and ubiquity of their coverage.

The first story in this section reveals not only the ónormalisedô use by an employer of checking social media such as Facebook (FB) in selecting candidates for positions, but admits to personal prejudice in so doing, e.g. political allegiances. In reality, the influence of subjective personal prejudice is probably prevalent, but not admitted to, in virtually all checks made on social media in the recruitment of employees:

> *ööOnce I should have employed a person in my husbandôs company, so beyond the CV I looked for information about him on Facebook (FB). For instance I check the political opinions (I have many friends who are directors in big companies and they notice that the employees that are too much left-wing oriented usually are against the company owner) (é). I agree with this system of selecting the human resources, as on the Internet you can collect info about his behaviour, if he is a reliable person or the friends he has,. (é) I check also if he writes on the Internet faked information about himself during the interview and I check if he says the truth on his FB profile. (é). Although I refuse to employ a person on the exclusive basis of the FB information and I match them with the info collected through the interview, but I evaluate the person also on the basis of practical motivation for the company (job experience, competence, etc.). At the end we did not employ this person but the motivation was beyond the FB info and the interview itself... I would do the same with other candidates, I check also when I select friends: of course it is more reasonable to select a candidate at the workplace, rather than to select a friend. It is a further ñtoolò, beyond the CV and references from the previous companies he worked for to select a person, it is a further infoô channel on the person. Once the person is employed I do not check anymore on FB, unless he has strange behaviours. Last week on the radio there was a speaker talking about big companies that usually have a psychologist to manage the interview for selecting candidates and they also check the FB profile of the potential candidate, although I haven't a big company, I agree with this system for profiling the person you are going to interview and potentially employ.öö*
>
> (Interview ID 206, 49 years, female, Italy)

What this story nicely demonstrates is the blurring of private and public spheres as a consequence of living in virtual or cyber space. New social media like Facebook make highly personal information easily available but at the same time the question arises whether this information should be considered private and personal since it is openly accessible by anyone. What is affected here are the strategies of identity management: being exposed to a situation like an interview when applying for a job, there are typically a number of standard data provided, such as information about prior employment record, qualifications, degrees etc., all documented in written form. The applicant can refer to this information producing an account of him/herself as a competent person, qualified for the position advertised. With access to

[259] Wigorts Yngvesson, Susanne, The Boss as Big Brother: Moral Aspects of Workplace Surveillance, in Gudrun Vande Walle; Evelien Van den Herrewegen and Nils *Zurawski (eds.), Crime, security and surveillance: effects for the surveillant and the surveilled*, Eleven International Publishing, 2012.

other sources like Facebook this situation changes. From the employerôs perspective this is simply an easy to use additional source of information, while for the applicant there is a loss of control over the way s/he wants to present his/her personality in the given situation of the interview.

Learning to live in the world of social media requires active and continuous privacy management in virtual space. Adjusting oneôs privacy settings and being aware of who might have access to information becomes part of daily routine as can be seen in the story below:

> ó*Well, you have to be realistic. What can be done, will be done, thatôs the way it goes with available technology and information. Who would stop an employer to google and find the information that is there? At the end of the day it doesnôt matter what I or we think about it. As long as we arenôt that stupid to call in sick and then post party pictures on Facebook (that kind of stories you hear about) thereôs not that much to be worried about, right?*
>
> (Interview ID 940, 46 years, male, Austria)

The use of social media at the workplace can create different techno-social dilemmas. What can be done, what is acceptable and how social media may be used, becomes an issue to be negotiated among workers and management. The story below concerns the somewhat odd phenomenon of the establishment of workplace norms for what could be termed ôacceptable deviant behaviourô, i.e. use of the Internet and social media, which appears to be tolerated by management provided the use is not excessive:

> ñ*Our online behaviour is monitored. They are interested in the amount of data we use. So if you watch videos on YouTube, then your data traffic is bigger than just reading some articles. I know that somebody watched two hour long videos on YouTube and then they came and told him not to do that. He did not really get into trouble, but it slows down the network and then people canôt work properly. We donôt have any websites blocked; they donôt really care about what we do online as soon as we get our work done. So if I watch too many NFL highlights videos, than I try to watch less videos on YouTube, I donôt want the traffic to be too big.*ñ
>
> (Interview ID 731, 25 years, male, Slovakia)

What becomes obvious in this little episode is the full integration of new social media in the work process, the blurring of private and professional use of the different communication channels and the way in which this can be negotiated in a consensual way among management and employees. At the same time the potential for more or less sophisticated, intrusive and encompassing surveillance practices becomes obvious.
A strategy of adopting informal regulation in those workplace settings where social media are used in daily routines seems to develop:

> ó*It is quite different, nobody monitors anything. As long as we are effective and do our work my boss does not care whether I take a private call, or check my email. It is actually helpful in my HR work, I use Facebook often to network in order to get some candidates for jobs. I do this strategically, when I need to ask whether my contacts*

know someone, I will change my settings in the Facebook, so anyone can see my posts, after I am done I change settings back to my very close and limited group of friends.ÕÕ

(Interview ID 585, 22 years, female, Slovakia)

Given the extended use of new social media, management has, in principle, access to a wide array of facts about their employeesô lives. Depending on whether management is trusted or not, the positions taken can vary greatly as the assessment of human resources managersô practices in the quote below demonstrates:

ÓÕ(I) Think it is terrible. No HR manager should do that. It is a real abuse of peopleôs private lives. What they do is not relevant and should not be taken into account unless they have committed a crime or racial abuse. Employers are unscrupulous finding out if applicants were in clubs until 3 am, also looking for political affiliation or sexuality.ÕÕ

(Interview ID 901, 24 years, male, UK)

As David Lyon observes: *ÓSpecialized knowledge strengthens the power of each modern agency, and taken together they seem to colonize ever-increasing tracts of so-called private life.ÒÔ*[260]

Depending on the practical organisation of specific types of work, surveillance can become extremely intrusive affecting every step an employee takes. A typical case is the story of a public servant who is patrolling the streets to enforce parking restrictions in a city in the UK. Here the term techno-social hybrid can be clearly applied:

ÓÕClocking in, signing-in and signing-out, there is a CCTV camera at the entrance to our office, body-worn CCTV cameras, hand held units and mobile phones. The body-worn CCTV camera records video and audio, and is used with a hand-held unit and the mobile phone. The body-worn CCTV camera must be switched on at all times ï it is meant to be for health and safety reasons, but management want to use it to deal with complaints. The mobile phone is used as a lone worker protection system ï you have to phone in each time you change location. The reaction of the public has not been good to the signage on our jackets advising that CCTV was in operation ï I expected it ï but not the experience I had last week where a mother went to the police to complain that I had taken images of her child.ÕÕ

(Interview ID 157, 44 years, male, UK)

5.2.5 Regulating privacy, trust and fairness at the workplace

Most national governments in the European Union have passed data protection and data processing legislation or codes to help define the boundaries under which public and private bodies may operate in relation to handling data, and indeed many have created regulators who issue guidance and investigate possible breaches. Within the workplace, responsible

[260] Lyon, David, *The electronic eye: The rise of surveillance society*, University of Minnesota Press, 1994, p7.

employers have produced a code of practice (or conduct) which attempts to define what is acceptable and unacceptable use of technology both within and outside the workplace, for example some may allow limited personal use of the Internet (using the employerôs technology/network) provided that this is carried out at lunchtime or in the evening and does not involve anything which could cause offence, such as harassing other employees, looking at inappropriate websites or sharing information or jokes which contain discriminatory, racist, sexist or homophobic material. Other employers may take a much stricter determination of what is óacceptableô depending perhaps on the type of business in which they are involved. Some quotations refer to a degree of common sense being required when considering oneôs own online and communications activities either in the workplace or outside the workplace when using the employerôs technology or networks.

Whatever the regulations at the level of black letter law, at the ground level of social relations between employer and employee the final decisive factor is trust. In our interviews we found a number of moral stories, contemplating the ñrightò and ñfairò way of handling the problems emerging with modern technologies in work place settings. The resource of trust shapes the way in which available technology is applied also from the management perspective, although surveillance technology sometimes appears like the iron fist in the velvet glove: it is there, it can be used, but as long as daily business runs smoothly and management has no indication of any wrongdoing, it will not be applied. In the stories below the notions of duty, fairness and mutual trust are invoked to describe scenarios for the adequate and reasonable use of surveillance technologies.

> *ôôEvery employee and every employer should know his rights and duties. See if I make private calls using my companyôs phone or if Iôd surf the web with my companyôs computer, or if I do take care of my private stuff at work, I have to face the consequences, then Iôll get a real óbollockingô (reprimand) from my boss. The employer has the right to control. But when the employer enters my private sphere outside my working hours, there I have no understanding for employers. From 9 to 5 it is ok, but I have the duty not to abuse the companyôs phone for private talks or to misbehave at work. The employer on the other hand has to respect my private sphere. That is how it has to be. Every employee who is a good employee and wants to keep his job would bear a lot of measures from their employer.ôô*
>
> (Interview ID 361, 69 years, female, Austria)

The scenario unfolding in the story above of an employer respecting limits of privacy is mirrored in the account of a manager detailing his companyôs policy with regard to surveillance, based on a kind of three-stage incremental approach to undertaking surveillance, should the need arise. This employer is acting quite responsibly and fairly in their attitude to trust and surveillance, i.e. that surveillance is not undertaken on a óblanketô basis of coverage, but occurs rather when the need arises:

> *ñWhen it comes to oversight of our employees, we have a working relationship based on trust. But we have several ways we can monitor the way our field employees ï representatives ï work. The first option is GPS tracking, people have GPS in their cars and we could use them to see where they drive and who they visit (doctors in*

certain towns). We do not use this GPS monitoring but it is very common among other pharmaceutical companies. We never used it because it is another paid service. But this could show you complete movement of the car. Our employees have to use software, where they put in information about their daily work ***ï*** *who did they visit and so on. Based on this information, the sales area manager can contact the person the representative visited, get some feedback and also find out whether the representative really visited the place and whether he was doing his job correctly. The third option and this is the one we used maybe twice in past 15 years and we did it only because we had a strong suspicion, is the monitoring of mobile phones. We had a suspicion that these people did not go to work, did some personal trips during their work hours, so we contacted the mobile phone operators and got information about their movement.****ò***

(Interview ID 742, 53 years, female, Slovakia)

While mutual trust is seen as a basis for good social relations it has to be acknowledged that trust and fairness are rather soft concepts and hence a realistic perspective should be taken when it comes to surveillance. The management reserves the right to use surveillance technologies and employees know that taking precautions is a safe bet. Whatever the legal regulations or the trustful relation between capital and labour, in the final analysis, as this last quote shows, it is better to take precautions.

5.2.6 Conclusion

Surveillance at the workplace can take on different forms depending on the kind of setting. From the perspective of the actors involved there are different ways of integrating new technologies with high surveillance potential into their everyday work life. One option is to develop a moral perspective, justifying surveillance practices as an adequate means to identify wrongdoers, to develop an adequate system of rewards and to improve health and safety of the workforce. Understandably this narrative is used mostly in stories told from the perspective of the ñwatchersò, i.e. management. A moralistic approach to surveillance can go either way, supporting and justifying the use of technology or criticising and condemning it. A key concept in either case is trust. If trust prevails, there is no need for surveillance; if surveillance is introduced this erodes trust.

Having to work in an environment under surveillance produces a number of practical and discursive strategies of normalization. Employees are aware of the fact of being surveilled in sometimes rather complex ways, but they learn to find ways to either work around the surveillance regime or to adapt their routine practices. What can be clearly seen is how the introduction of new ICT in work processes changes the situation of employees dramatically and how new rules and regulations, formal and informal have to be negotiated and implemented. Those who grew up with new social media have acquired the skills to adapt their behaviour when using e.g. Facebook. They are aware of the pitfalls of documenting their private life online.

What could be shown in the stories about workplace surveillance is the wide array of technologies and strategies deployed here. From crude and simple CCTV cameras installed on the premises to highly sophisticated multi-channel and multi-sensor systems tracking every move across multiple sites and assessing performance using several indicators.

The changing structure of the workplace and working environment in recent times has been accompanied by greater flexibility in how, when and from where employees conduct their employersô business. Greater flexibility has been encouraged by employers through facilitating flexible workspaces, home working, provision of laptop computers, smartphones and other technologies to allow businesses to respond to the 24/7 demands of the modern working world. However, accompanying this more flexible approach by employers, and apparent weakening of previous monitoring controls, which they might have used to ensure that employees were performing to required standards, there has been an increase in the availability of surveillance technologies, which can and are being used in the workplace. Many examples of the different types of workplace surveillance technologies being used are provided in the stories, including the most direct: body-worn CCTV. Some evidence of the resilience of employees is provided, through resistance to the practices of management, or indulging in deviant behaviours. Coupled with the increase in flexible working has been a massive rise in the use of communications technologies, including the Internet and social media, all of which are being used in both professional and private settings. This has resulted in what has been described as a óblurringô of the boundaries between the private and the personal, which then invites an ethical debate around these issues. Many governments have produced legislation covering data protection and data processing, and most have appointed regulators to try to manage the inevitable interpretations and sometimes conflicts which arise, although in reality the legislation can never be expected to keep up with the speed of technological change. In the workplace, many responsible employers have produced codes of conduct for employees around use of the Internet and use of employerôs hardware and software when not on working time, and provided definitions of what is acceptable and unacceptable use. Above all, a fair degree of common sense is required from any employee engaging in what might be regarded as ópersonalô activities while on ówork time.ô

Call centres are popular with governments and development agencies due to the labour intensive nature of their staffing requirements, and impact which they can have on unemployment levels, however as can be seen from the interviews and the literature, they also create environments which are target driven and feature what some might regard as ubiquitous and oppressive forms of surveillance monitoring. Due to the ubiquity and non-discriminating nature of the surveillance technology within call centres, this is claimed to have mediated the behaviour and attitudes of some employees (and supervisors) in harbouring resentment against some team members who perhaps do not meet the required standards, and in effect some managers may look at the statistics and not the underlying (and personal) reasons which might lie behind the output or performance.

Turning to ógoogleveillanceô and the use of social media in a recruitment setting, there are many examples provided from the interviews of employers using it to monitor the activities of employees, and as an aid to informing their recruitment decisions for prospective employees. There seems to be inevitability about the continuing growth in use of social media in this context, and to that extent, it could be regarded as having almost become ónormalisedô. Personal prejudices are also evident when using this medium. Reputational management is a key driver for many employers in justifying the use of social media or checking work emails to view what their employees have been saying. It is important therefore for employees not to be irresponsible and to write (publically available) disparaging remarks about their employer, their team leader or colleagues.

Regarding national trends in workplace surveillance within the countries where the interviews took place, i.e. Austria, Germany, Italy, Slovakia and the UK, it is difficult to draw firm comparisons, however it is clear that they all have a regulatory system at the national level for data protection and processing; they all respect the rights of personal privacy, and there is a role for some form of representation of employees through trade unions or works councils etc. when discussing surveillance technologies in the workplace.

Surveillance in the workplace, due to its ubiquity and omnipresence, is no respecter of the development of relationships. Regarding trust, it is the single-most important building block upon which future relationships, reciprocity, and mutual respect can be developed and strengthened. Time and again from the interviews, we were provided with examples of the breakdown of trust caused by management, most often simply because they used the data or images which the surveillance technology provided them with, which of course was too tempting (in their eyes) to turn down.
Often, the data and images were used for purposes other than those originally agreed upon, resulting in the breakdown in relationships, and sometimes increased resilience and resistance by employees to their employer.

In the final analysis it seems that there are no serious options for an active strategy of resistance against the rise of surveillance in the workplace. The only option is either to quit the job (only to probably find a new position where a similar regime of surveillance prevails) or to develop informal counter strategies to neutralize the surveillance practice to some extent. Since ICT is on the rise in most workplaces settings, be they industrial or service, it can be assumed that surveillance of work environments will become more intense across all areas and workers will continue to develop ï wherever feasible, morally justifiable and practically possible ï their counter strategies to work these systems in their favour.

5.3 SURVEILLANCE IN THE EDUCATIONAL SYSTEM

Alexander Neumann, Reinhard Kreissl

None of the interviewed citizens across the participating was directly asked about experiences with surveillance at school. Nevertheless, several stories related to surveillance and education were documented. Most of the stories revolved around routinized surveillance by means of technologies like CCTV or swipe cards for students to register the time of entry to the school building or the dorm. In some of the stories the headmaster or the teacher as a charismatic watcher was contrasted to the present-day routinized surveillance in schools. The feeling of being influenced or controlled by a supervisory person like the teacher is something most of the interviewees could recall and talked about during the interviews. The iconic figure of the dominant teacher they were referring to is a prominent icon that can also be found in popular culture. One could think of the teacher in Pink Floyds music video for the song ñAnother brick in the wallò from 1979 where a teacher in a traditional British school uniform with a wooden switch is standing at the gate of a school waiting for the pupils.

5.3.1 Charismatic panopticism or the headmastersô ritual

Besides technologically mediated surveillance and the charismatic panoptic type of surveillance, two other types of school surveillance stories were identified. We identified stories of pupils being watched and expressing the malaise of being a student and stories of teachers watching students and expressing the impossibility of herding óyoung rascals, both of which were very common. An additional story describes a headmastersô ritual:

> ñ*Once the headmaster wanted to know whoôs coming late to school. He only thought about the pupils not the teachers. So he locked all doors and waited outside the school to welcome those pupils who were supposed to be late. It was like 5 minutes before the first lesson would have started at 8am. He stood at the school gate for a while, then he recognised that that even some of the teachers were not at school after 8am. He was a kind of old fashioned, a true headmaster. You donôt find these kind of headmastersô anymore today, today they are way more liberal and moderate.*ò
>
> (Interview ID 281, 72 years, female, Austria)

What is described in this anecdote is literally an old fashioned form of surveillance. Although one could develop a reading of this story as an uncomfortable measure, both for the teachers, who are normally in the more powerful position of the watcher and are now being watched by the headmaster, and the pupils, this story provides a good example for a common technique of neutralization used to cope with surveillance. This technique can be called the legitimacy of power or the Eros of the watcher. The headmaster as described in this story is an old fashioned powerful male person of respect and authority. In the context of the story, he is the only one able to stand at the gate and wait ï or better watch ï for the other actors in the story. In the setting of the story a traditional type of authority is attributed to him, almost in a Weberian sense of charisma. The power of the watcher and his ability to control a large group of pupils and teachers on his own is not made possible by technology e.g. a CCTV control panel in his office, but rather the traditional headmasterôs ability to control others rests on his physical presence at the school gate. He is described as an authentic leader, or in the words of our storyteller a ñtrue headmasterò. This perception of the charismatic leader who is capable and entitled to watch others because of the charismatic authority ascribed to him is the opposite of a modern management executive.

It is extremely difficult to account for privacy labour in settings in which the watcher acts as a charismatic and authentic leader. To contest the authority of the charismatic leader and to develop resistance or resilience against the surveillance regime of the leader would be most likely considered deviant behaviour. The story does not end with a twist where the pupils or even the teachers stand up against the headmaster and demand more trust, that they show up at school or work on time. The story concludes with an almost nostalgic statement that headmasters nowadays arenôt like that anymore. Today they are ñ*way more liberal and moderate*ò. Today the headmaster would have had access to CCTV footage to watch pupils and teachers coming late or he would have access to a database in which tardiness is documented and stored.

5.3.2 Routinized surveillance in schools using technology

A contemporary headmaster waiting for pupils and teachers at the school gate would be considered *old fashioned* with a negative connotation and the story would probably contain justifications for this *old fashioned* behaviour. Indeed the fact that CCTV is being used to monitor students was raised in several other interviews touching on the issue of surveillance in the educational system, particularly in Italy where video-surveillance at schools has become a highly controversial topic over the past 10 years. The previous quote reminds us that teachers are not only and exclusively in the role of watchers, they are also watched, although in times of electronically mediated surveillance the attention of the electronic eye is focused on the students. The school in the next story recently decided to install CCTV cameras to protect against vandalism. The teacher telling this story was sceptical about the effectiveness of CCTV as she mentioned that on the whole, the teaching staff knows who is responsible for vandalism at her school. In this story it is no longer the headmaster waiting at the gate for the pupils and the other teachers, but rather the CCTV camera that is installed at the gate.

> *ñI worked in schools where there was CCTV and in one specific case video surveillance was on school buses to stop bullying. Usually CCTV was at the entrance of the buildings. A few years ago surveillance cameras were installed to protect a school against vandals after teen vandalism had occurred. This really annoyed me as I felt spied on and I didnôt get why they put up the cameras. We all knew who did it [who vandalized the school] and I donôt think CCTV is a deterrent. We have to deal with social unease in a different way. The city council didnôt explain anything to the parents, they just installed the cameras. By the way, the parents were enthusiastic about it. ò*
>
> (Interview ID89, 52 years, female, Italy)

Although the effectiveness of CCTV to prevent future acts of vandalism is called into question, the story provides a good example for the inescapable character of modern video surveillance systems. It is not only the potential perpetrators who are being monitored: the electronic eye is indiscriminately watching everybody and in that sense the CCTV camera at the gate has a similar function to the iconic headmaster in the first story of this subchapter, although considerably more effective.

5.4 RELATIONSHIP BETWEEN CITIZEN AND THE STATE

The relation between citizens and the state is the mother of all surveillance relations. The growth of public bureaucracies in the modern state is considered the dominant driver for the development of technologies with high surveillance potential. Being identifiable in a database administered by a public authority is the proto-typical characteristic of citizenship. Individuals are endowed with enforceable rights, duties and privileges only as more or less machine-readable subjects of the state. While on a daily level personal encounters between citizen and representatives of the state are strictly speaking rare, a plethora of daily routines take place in

the shadow of the Leviathan, as Spittler fittingly put it.[261] Whenever the lay citizen is requested to produce personal data for identification outside the realm of commercial transactions (like in online shopping) this can be perceived as an encounter with the state. The practical organisation of such identification encounters is affected by the kind of technology applied. Looking up a personôs name in a paper-based filing system creates a different situation compared to the barcode scanning of an identity document stored in a remote database. Last not least the digitisation of such procedures significantly lowers the threshold for setting up checkpoints where citizens have to demonstrate their eligibility goods, and services.

5.4.1 Citizens experiencing being controlled by the state

In this subchapter we deal with citizensô experiences of being controlled in various encounters with the state. The constellations presented here, involve individual citizens encountering some sort of public or state authority, be it the police, security personnel at the airport or any other type of public servant. Beyond such face-to-face encounters, citizens also reported concerns of being treated as data-doubles in virtual databases.[262]

The first story addresses the imbalances or perceived injustice of data collection and control by state authorities. While the need for data collection or surveillance measures is not totally rejected, the fact that surveillance practices are unevenly applied is seen as a problem. The basic logic of the first quote is straightforward. Being exposed to controls is acceptable as long as these controls are perceived as being effective and evenly applied to all subjects in a given situation.

> *"It happened at the airport in Dubai at least 6 or 7 years ago, but it was after the 11. of September, we went through, sitting in the transit area, there was a negro sitting next to me. She checked in and was examined like me, and she manicures her fingernails with a razor blade. Well, we see what still goes through. Therefore, it makes no sense to control for dangerous objects.***ò**
>
> (Interview ID 48, 55 years, male, Austria)

Surveillance measures and practices by public authorities are deemed acceptable when the surveillant gaze extends symmetrically to both sides: citizens and public authorities. Surveillance can also serve as a means to document encounters and conversations between state bureaucracy and its citizens. Such documentation, based on recordings of telephone conversations, like in the story below, can provide evidence to be used by the citizens when they feel improperly treated. Surveillance here is an element of a bureaucratic culture: every act, event or encounter with bureaucracy has to be documented and filed. A recurrent argument running through the interviews is that in a democratic society such documentation should be made available to both sides: the organisation and their clients. If this symmetrical

[261] See Spittler, Gerd, Streitregelung im Schatten des Leviathan : Eine Darstellung und Kritik rechtsethnologischer Untersuchungen. *Zeitschrift für Rechtssoziologie* Jg. 1 (1980), H. 1, S. 4-32.
[262] Haggerty, Kevin D. and S. Ericson, ôThe surveillant assemblageô, *The British Journal of Sociology*, 51,No. 4 2000, pp. 701ï 717.

relation is violated, this has a negative impact on trust in institutions. Surveillance is seen as an illegitimate practice if done incompetently or applied in a one-sided manner, as highlighted in the story below.

> *ñYes, in fact it was a conversation I'd had with the County Council and I'd felt that I'd been treated in a bad way on the phone and I wanted a recording of the conversation. I told them I was entitled to that recording. Two weeks later I got a CD of the recording but the sound quality was appalling; you couldn't hear anything. And at the time I felt cheesed off because, by law, I know that the local authorities have to record all local conversations and I couldn't take further recourse to make a complaint.*
> *Legally I knew I was entitled to ask for information. But I did get it. It took a long time to get. When I say a long time, it took ten days but it wasn't a viable recording so I wasn't quite sure if they were fulfilling their end of the legal bargain, if you like.... I was satisfied that they were prepared to do that. And, as I said, I didn't do it as a threat but the conversation that I'd had with a certain individual, I thought had been extremely rude and aggressive and at the time if I had had a clear recording I would have taken it further, but as it was the integrity of the recording was very poor so you couldn't hear anything.ò*
>
> (Interview ID 46, 44 years, male, UK)

Trust in institutions is a major resource when it comes to the acceptance of surveillance measures. If law enforcement institutions do their job in a professional manner, surveillance is acceptable to a certain extent. However, a tipping point is reached when thresholds for data collection are so low that anybody can indiscriminately become an object of police surveillance activities. Forcing ordinary citizens to provide their data under the pretext of a generalized suspicion is regarded not acceptable and creates a feeling of powerlessness. Providing personal information in an encounter with a police officer based on a reasonable request to provide this information is perceived to be an acceptable practice. This is different from a situation where personal information stored in databases is processed without knowledge of the individuals involved.

> *ñI can see the problems with it, but I also think thereôs a fair amount of truth in that I feel pretty secure, I suppose. At the same time, I donôt think the state, the police, or whatever, has a right to look into every aspect of peopleôs lives for no reason other than fishing around for issues. I think itôs okay for the police or authorities to look into something if it arises, and look at all sorts of data, as they do, but I think as a matter of forceé That's what seems to have come up recently in the news, that they are doing this as a matter of force, and Iôm less comfortable with that, obviously.ò*
>
> (Interview ID 64, 43 years, male, UK)

What many stories demonstrate is an understanding of ñthe stateò as personalized. Encounters with police officers, IRS-personnel, social workers and civil servants and data collection activities are acceptable to a certain degree. This changes completely, when these faces of the state vanish and are replaced by technology or technically mediated forms of interaction. The symbolic or personal representation of state authority can be compensated for by a high level of generalized trust in the state as institution and provider of services and (public) goods such

as security. In a situation of trust, state surveillance measures are accepted and perceived as effective and legitimate. The standard pre-emptive reasoning of *better safe than sorry* lets surveillance appear as a solution to problems of crime and security. Citizens following this line of reasoning are willing to trade in their privacy for a presumed gain in security and protection against criminals, as demonstrated in the following stories.

The overall idea informing these stories is that surveillance increases the security of the citizen. Citizens consider themselves exposed to more or less threatening individuals in different situations and that threatening individuals will be identified and identified through surveillance measures.

> *ñWe want to be safe at night and everywhere, but we are against cameras. We want terrorists to be recognized and arrested, but we don't want to be monitored. I mean this is not how it works, right? é And how much they've prevented already, I don't want to know it. So if they want to monitor and wiretap me: Go for it.ò*
>
> (Interview ID 311, 55 years, female, Germany)

> *ñFor example, take the airport. I always travel with my kids. If I had to give my fingerprints as an additional security measure in order to prevent, for example, kidnapping I would do it. This wouldnât violate my privacy. At banks or hospitals where access control is very important, more surveillance is not a problem to me. I would also increase access control measures at schools through CCTV at the entrance of schools and also at the entrance of classrooms. CCTV is not that invasive and it is useful ex post.ò*
>
> (Interview ID 575, 40 years, female, Italy)

> *ñI don´t notice cameras in public places at all. I donât care and what am I supposed to do anyway? I think that the idea of it is great! I want to be protected and I feel very comfortable with it. Let everybody see me, I donât care. It serves the public good and better security.ò*
>
> (Interview ID 673, 26 years, female, Slovakia)

> *ñI guess, my logic is that the government are tight on money, so they wouldn't just randomly pick your conversation and just listen in for fun; they do it for a reason. é If it's for a just reason, then I'd be fine with it, but that does make me a bit uncomfortable because you think it's private. If I was committing crimes the whole time, then I would mind, but I'm not, so I don't really mind. I just feel like it's taking it quite far, but when the raids and stuff were going on in London a couple of summers ago, didn't they realise that was going to happen by tracking people's BBMs and texts, so that does make me think that it's serving a purpose and that it's good, so I don't mind as much.ò*
>
> (Interview ID 915, 18 years, female, UK)

The subtext in some of these stories is interesting as it suggests a clear difference between the law abiding citizen who has nothing to fear and gladly gives away his/her personal information and a group of unidentified (but identifiable) wrongdoers who can be detected by massive surveillance and control. There is the implicit assumption of a powerful and benevolent state capable of identifying wrongdoers by means of surveillance.

5.4.2 Data collection and data retention

In April 2014 right after IRISS completed its empirical research phase, the European Court of Justice declared the EU Data Retention Directive invalid. From March 2006 to April 2014 the ñDirective 2006/24/ECò allowed for citizensô telecommunications data to be stored for 6 to 24 months. The directive enabled law enforcement agencies to request data from telecommunication service providers such as E-Mails, IP-addresses, phone calls etc. During the interviews most respondents were aware that there is such a law in place, and some expressed rather critical views on the directive.

> ñ*I donôt want people to know about my medical history. I donôt want them to know when Iôm travelling abroad. I donôt want them to know my opinions. I donôt want them to know all sorts of private things. Why should this wonderful system know my beliefs whichever label that is, political, social, sexual. Look at the attitude towards the gay community. In 40 years itôs massively changed. That doesnôt mean in the next 40 years the attitude towards a minority or a majority could change. I always used to say to friends, look, in Federal Germany the Greens, the former Communists, are part of the government. And no doubt the Germans at one stage collected intelligence on the Greens, even though they wereé I donôt know why, but they did. But theyôre now members of the governmentò*
>
> (Interview ID 393, 60 years, male, UK)

Here the respondent raises concerns about the fact that data can be stored for a very long period of time. Even if it remains unclear what is to be done with this information and by whom, it raises the awareness of citizens ï the fact of data being stored for any form of future processing creates substantial unease.

The next story draws a comparison between ñ*the good old days*ò before communication and data storage technologies and tools became elements of everyday life and the present day. Asked about his opinion on the data retention directive, the respondent did not see a need for a general rule to store data as citizens often ñ*give their data away*ò anyway. He sees a function creep in social media platforms such as Twitter or Flickr where one can share images with the rest of the connected world, including law enforcement agencies who in this case do not need a data retention law for their investigations, as the necessary information is readily available.

> ñ*When there's a major incident, if you think back to our youth, the good old days of rioting. When they showed a film, everyone was throwing things at the police. You look at the riots now, half the people are throwing things at the police. The other half have their mobile phones out, taking photos.... Now, those photos are going straight onto Twitter, they're going straight onto Flickr, so if you're the police, rather than rushing around trying to identify who's there, go on a few websites that look at the geo-location markers from different information and say, who was there taking photographs on that night. And you can see all the photographs being uploaded.ò*
>
> (Interview ID 405, 50 years, male, UK)

The next story is located in Austria, where a long and controversial public debate about the data retention law took place, before finally, in May 2014, the Constitutional Court in Vienna declared the law invalid. Here the respondent is rather sceptical about the fact that personal information about her is being stored and is, in theory, accessible to state authorities such as the police. She was aware about the present situation in Austria and also saw a clear trade-off in this respect ï a trade-off that does not always work to her personal advantage. If citizens nowadays want to participate in electronically mediated forms of communication they more or less have to agree to their personal data being in some form. This quote also shows the inevitability of this practice, which creates great unease amongst many of our respondents. Most citizens know that communication data will be stored, although they are normally not aware by whom and for what purpose.

> *ĂIf I want to participate, I need to be willing to expose certain parts of my personal data. I myself determine where I disclose which data. The only thing that maybe annoys me a bit ï but I canôt do anything about it ï is that maybe somebody draws wrong conclusions based on my behaviour in the Internet that is of course recorded precisely. For example, the data retention law [in Austria], one knows what [who] I phoned, what websites I visited. There somebody looks it up in a [specific] context and says ôI see, madam XXX was there and there, then she must have done or planned this and that according to our profile.ôé that is indeed a little bit [unpleasant] é [but] I would not know how I could influence that. Whoever processes that [the recordings], it could be also a private person or an [research] institution. Who knows? I cannot assess whoever it is.ò*
>
> (Interview ID 179, 63 years, female, Austria)

For many citizens it seems to be rather unclear how the technology behind the data retention law is operating. Questions, such as ï are entire phone calls being recorded and what is going to do with all this information? ï were raised by several respondents. Finally the fact that communication is been recorded also leads to further considerations about becoming an active member of the civil society (e.g. what is being recorded about me when Iôm participating in a demonstration).

> *ĂNot directly, but all that data retention of my mobile phone, that's not happening to really do something right? They just collect and then "Let's see what we can do with it". But maybe, I don't know may my presence at a demonstration has been recorded via my mobile phone. Not to judge me, but they know it.ò*
>
> (Interview ID 274, 33 years, female, Germany)

Many of these stories report a Kafkaesque experience: we do not know what happens to our personal information once it vanishes in cyber space. Someone may do something with this information that may have unforeseen consequences in the future. For some respondents, data collection by public authorities seems legitimate to a certain extent, although any form of outsourcing or private data collection is consistently considered illegitimate.

> *ĂThis is not legitimate. There are problems with companies developing face recognition software ï this should be done by public officials. The police for example*

should not be sub-contracting this type of work to companies, which have less control and accountability. Using Facebook or Twitter to record crimes should not be a first resort. People accused of a crime are innocent until proven guilty. This accuses the person and causes a real problem with the judicial process, and of proving guilt.ò

(Interview ID 153, 44 years, male, UK)

"I know about a case when footage was used in case of rape in my city, so for me it makes sense to have public CCTVs, but I do not trust private CCTVs, I do not think there is enough control and accountability that is there with public CCTVs.ò

(Interview ID 587, 22 years, female, SLO)

For other respondents, the presumably unprecedented and uncontrollable policies of collecting and processing data, makes the state look like a ñbig fishing netò indiscriminately sucking in data around the globe. This feeds into dystopian views leaving no room for civic action and resilience is equated with surrender.

ñI think the fact that you have branches of governments who are collecting information on people. For a start, itôs all just a net. Itôs not like they talk about how software picks up code words or that specific phrase. Thatôs bollocks. Itôs not because they are justé Itôs just a great big fishing net and the fact that itôs being operated in such a way that, as I said previously, weôre collecting the Aussies, the Aussies are collecting the Yanks, the Yanks are collecting the New Zealanders, the New Zealanders are collecting the Canadians. Itôs, like, pull the other one. If it were targeted, youôd be collecting your own, but itôs not. Itôs Tempora, isnôt it, that does it here?ò

(Interview ID 227, 43 years, male, UK)

Embracing this dystopian global view leaves no room for deliberation. It should be noted, however, that this and similar views are in the minority. In many cases citizens are aware of what the state is doing, what its capabilities are and that any legal restrictions can be overruled if it is deemed necessary in a presumed or real state of emergency.

5.5 CONCLUSION

Running through this chapter was the question of fairness, trust and surveillance from the perspective of citizens as members of the work force, clients of the educational system or simply as plain lay citizens in their multiple relations to the state. Trust and fairness are important resources shaping citizensô attitudes and actions. Trust operating in the background, i.e. without being questioned or closely scrutinized provides for ontological security. Erosion of trust breeds surveillance and being under a surveillance regime erodes trust. This mutual dependency amounts to a vicious cycle. As the chain of events unfolding in the stories demonstrated, it is often impossible to evade the surveillant gaze and if so only at very high costs (such as giving up a position or risking severe sanctions).

This cycle can be broken when the notion of fairness is introduced. The notion of fairness is a guideline to determine when surveillance may be justified. It provides a measure of what can be deemed acceptable and what is perceived as beyond any reasonable limit of intrusion into

the private sphere. Striking a fair deal is a baseline for every controversial constellation of surveillance. Any attempt to negotiate surveillance regimes invokes the idea of fairness in one way or the other. Taking a fairness perspective, the standard trade-off model can be translated in a different discursive frame, introducing fairness as a third element. Any suggested invasion of privacy for the sake of increased security has to undergo a kind of ñfairness testò to determine whether the burdens of surveillance are adequately shared, whether other options might be feasible or whether ï as often seems to be the case ï the cure is worse than the disease. The simple and blatant move ñé because it increases securityò no longer is considered a legitimate and sufficient answer, when fairness is introduced as a criterion. While fairness is not often mentioned explicitly in the stories from the interviews, it can easily be invoked when reconstructing the underlying mundane ethical reasoning applied in the narrative accounts. Citizens are willing to accept being exposed to surveillance when this happens in a fair and even way. They develop dystopian or negative views only when there is no other option and they lose all control over the situation to which they are exposed as surveilled individuals.

6 5TH DILEMMA: ENGAGEMENT AND SECURITY

William Webster, Charles Leleux

6.1 INTRODUCTION: DOING SECURITY, CITIZENS WATCHING CITIZENS

The analysis of ócitizens watching citizensô (CWC) and neighbourhood watch (NW) has been written from the perspectives of first, careful examination of peopleôs óstoriesô taking into consideration the context and settings in which they have relayed their account, and in particular whether or not their story is a descriptive and factual account based on real-life experiences, or rather a normative one which is based on their feelings and opinions; second, consideration of the stories and their relation (if any) to the discourse around contemporary surveillance studies and surveillance theories, i.e. are the stories merely reaffirming what we know already about the discourse and theories, or are they telling us something new; third, examining what the stories are telling us about the negative, positive or ambivalent attitudes arising towards CWC and NW; fourth, comparing the national practices and trends in CWC and NW in those countries from where participants were interviewed and from where national case studies were carried out (Austria, Germany, Italy, Slovakia, Spain and the United Kingdom), and finally, the identification of three ómaster storiesô which highlight the key dilemmas which are emerging around the issues of NW surveillance, democratic accountability and governance of NW, and the societal, cultural and historical reasons which have influenced the growth of NW or its lack of development. This contribution is intended to help inform the European Commission, wider academic, policy-making and practitioner communities when considering CWC, NW and surveillance in the community.

CWC carried out through NW is usually done covertly. It is an example of community-based resilience in response to localised or societal problems (or issues) such as theft, anti-social behaviour, fear of crime, bogus callers or simply an example of community solidarity amongst people who share similar values and have common concerns over personal security and welfare. Surveillance undertaken through NW is not normally negotiated or regulated and is not subject to any conventional forms of governance controls. It often represents an asymmetrical power relationship in which the power lies with the ówatchersô, and the ówatchedô are powerless, most likely being unaware about when, where, by whom or how they are being surveilled.[263] The ówatchedô will commonly not have been consulted, and therefore will not have had the chance to participate democratically in the process, or to have had the chance to discuss whether or not they agree to have this form of surveillance in the first place. Consequently, the right of the ówatchedô to be anonymous has been removed unilaterally as has their right to personal privacy. The persons carrying out the surveillance will probably not have been elected democratically or be subject to the usual rigours of public accountability, and the democratic legitimacy to undertake NW surveillance is therefore questionable, and to this extent it could be described as a community óharmô due to the fact that the ówatchedô do not have a say in almost any aspect of its conduct. NW volunteers will not normally have been subject to any criminal records checks, and the trust and confidence, which communities may place in them could therefore be misplaced. On the other hand, the fact that citizens are willing to give up their spare time to help their community by attempting

[263] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, 2007, p. 23.

to prevent crime, or perhaps allaying the fear of crime, or by undertaking ógood neighbourô activities by looking after more vulnerable members of the community, demonstrates a commendable form of active citizenship or civic engagement. Stakeholders include local communities, community groups, public bodies including utility and transport organisations, elected politicians, the police, and local and national governments. Limited evidence was found about the use of technologies in undertaking surveillance through CWC, although examples of the use of websites for NW were observed. The national co-ordinating bodies for NW in the UK use a NW Alert Notification System which allows them to send out email alerts to all of their registered contact persons, allowing national dissemination to potentially thousands of NW members in a very short space of time.

No óshocksô were evident from the survey results from each country, although tensions were sometimes found in communities, which were experiencing either temporary or longer-term difficulties with integration, for example, of marginal Roma communities and the majority indigenous populations in Slovakia, and the consequential stigmatisation or re-stigmatisation of these groups. Further tensions were seen in Austria, Germany and Spain, due to their former authoritarian pasts, where sometimes the media, the police or politicians raise fears over the potential right-wing tendencies of NW groups. The authoritarian pasts of some countries, coupled with cultural traditions of respecting authority, has had a major influence on the low levels of growth of NW, compared to say the UK, which has experienced significant development of NW. Best estimates of the current numbers of registered schemes in the UK, provided by the national co-ordinating bodies in 2013, are England and Wales (12,324); Scotland (1,600), and Northern Ireland (776). The British Crime Survey estimated that in 2006/07, 16% of the UK population was covered by a NW scheme (which equated to 3.8m households in England and Wales).[264]

Examples of óactive citizenshipô and ócaring for othersô are to be found in many of the countries from which quotations are provided. One of the most common themes emerging is a lack of faith in politicians and in some cases the police to tackle perceived or actual societal problems such as burglaries, bogus callers, and fear of crime. This is one of the factors, which have resulted in communities or individuals showing collective resilience and taking on responsibility for watching over each other, and each otherôs properties, and in so doing self-empowering themselves. This self-empowerment includes the use of power to monitor members of their community either with, or more likely without, their consent. Lyon makes the following point with regard to surveillance and power: ó*Surveillance is always bound up with questions of power and its distributionéô*.[265] Some examples demonstrate the desire to look after each other in a caring and humanitarian sense, which has probably grown stronger as the members of the community have aged. The actions (including surveillance) which are then undertaken are arguably not sanctioned in a formal sense or approved by any authority, other than perhaps registering a neighbourhood watch scheme with a national co-ordinating body, and establishing communications channels with the police and other authorities. Carried out overtly, awareness of NW surveillance may moderate peopleôs behaviour or create a

[264] 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.
[265] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, 2007.

response from them, and in those senses the existence of surveillance and surveillance technologies undoubtedly has the ability to moderate or control peopleôs behaviour, reactions and opinions. Arguably, in the context of overt surveillance, citizens may feel that they have surrendered their right to anonymity and privacy.

Rather surprisingly, NW viewed as a ósoftô form of law enforcement, has developed outside the formal control of the police in all of the countries examined, although in some areas of the UK the police still maintain an active interest in supporting NW, although admittedly at a lower level than some years previously. However, in countries such as Germany and Austria the police have at times been unsupportive of the development of NW, and its growth across all countries could be seen as a community response, and indeed community resilience, to the failure of the police to provide the level of support, which communities expect. This may be too simplistic a view as inevitably there will be funding pressures on the resources of the police, and while a community may view crime in their area as being a really important issue, the police may interpret this as being very low level and regard the concerns as being more about the ófear of crimeô and may not allocate the resources which the community expects. Bannister[266] argues that NW in the UK has grown as a societal response to shared values within communities as opposed to responding to actual levels of risk and crime, and as a consequence police and local authority resources may have been distributed disproportionately to communities which have NW schemes with no particular risk of crime, instead of to those communities which may have had a greater need. The ways in which citizens engage with NW surveillance practices in the different countries examined through this Deliverable of the IRISS Project varies considerably, often due to cultural or historical reasons, and these are explored in further detail in the cross-country comparisons presented in this contribution. The policy discourse around CWC and NW is generally unexplored in most of the countries examined, with the notable exception of the UK, which differs from the other countries examined both in terms of the extent of the policy discourse around NW and the scale of the development of NW and its integration with UK society from the early 1980s to the present day.

6.2 CITIZENS AND COMMUNITY SAFETY

In this section we provide examples of a ócascadeô system of disseminating NW alerts which have the potential for reaching up to 5,000 households within a short space of time; the range of support services provided by the police in the UK in relation to community safety including an acknowledgement of the move away from giving advice primarily on prevention of crime to community safety, and details of the range of other community initiatives which a NW volunteer has engaged in. Regarding the final example, there is conclusive evidence from NW interviews in the UK that volunteers are active not just in their own NW group, but in many other community-based safety initiatives too.

[266] Bannister, Jon, *Cases of Democratic Resistance in Surveillance Society*, IRISS Consortium Meeting, University of Sheffield, 24-26 June, 2014.

The first quote is a story which presents a very positive view of surveillance in a NW context, and the impact which a simple telephone cascade system for NW alerts can potentially have for mass community (covert) surveillance of a regional population and its day to day activities:

> *ñNeighbourhood watch is not an identity on its own, itôs a point of reference to allow people to do what they want to do. Your neighbourhood watch is as good or as bad as you want it to be, active or inactive as you want it to be. In my region, there are 4 districts and we use a telephone cascade system to pass on communications. We have 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 beauty of the scheme is its simplicity, and co-ordinators will receive calls back to confirm that the message has been conveyed and cascaded properly. The system has the potential to pass a message on to almost 5,000 households within a very short time, if it all goes smoothly. It ensures that lots of eyes and ears are looking and listening. 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.ò*
>
> (Interview ID 171, male, 71 years, UK)

The benefit of this system is the speed with which an alert can be issued and hopefully disseminated, for example if suspicious white vans are seen in an area, although the drawbacks would be first, its reliance on each person in the cascade system being available and actually passing the message on, and second, the number of schemes which have not registered with the national co-ordinating body and therefore could not participate in the cascade system. It does however represent a potentially powerful example of community resilience on a regional scale, although the population being surveilled will be largely unaware that it is happening or have the opportunity to influence any aspect of it.

The second quote is a story from a serving police officer who has several roles in relation to crime prevention:

> *ñI am a Crime Prevention Officer, Architectural Liaison Officer and CCTV officer, and advise home owners and business owners on security, assess CCTV requirements, and also try to ódesign outô crime at the planning stages. If there are house break-ins, or unauthorised entry to business premises, or at schools, I will go and visit them and give advice about preventative measures which will hopefully mean that it does not happen again. I will also assess the surrounding area looking at street lighting, car parking, perimeter safety and then develop an action plan. Formerly, I would act as a Neighbourhood Area Crime Prevention Officer, sitting on a local crime prevention panel or community safety panel, often acting as the Secretary taking minutes and so on. 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. I still give advice to neighbourhood watch groups on what is happening in their area, and often this is then included in their neighbourhood watch newsletter. Neighbourhood watch co-ordinators still want Police involvement in their activities. New neighbourhood watch schemes which are registered with Neighbourhood Watch Scotland, have to have their scheme óstampedô at their local Police station. There are a number of schemes in my city which are both registered with Neighbourhood Watch Scotland and unregistered ï often, they donôt realise that they need to register in order to receive leaflets, notices and other advice.ò

(Interview ID 173, male, 42 years, UK)

What is striking about this example is first, the range of support services and advice which this dedicated officer provides across different disciplines, and second, confirmation of the changing national priorities of the police in Scotland from crime to community safety. The change in focus by the police towards community safety is also mirrored by NW groups over recent years in Scotland, and England and Wales.

The final quote presents a positive view of surveillance, community involvement and active citizenship, which includes NW:

ñI got involved having come from defence security. I was invited (by the Police) to become involved about 12/13 years ago. At that time I could only devote a small amount of time, but the Police asked me to help with their Neighbourhood Watch: Young at Heart initiative, to advise the elderly ï they gave them a free lunch, and explained current rights. I am also involved with the Community Speedwatch safety campaign with the Police, and Operation Nightlight, which is a home safety, intensive campaign - during dark nights it is an invitation to criminals (to burgle houses) between 4-6pm. We give advice to tourists coming off cruise ships ï how to get about and personal safety if necessary. I am the Chair of Regionôs Neighbourhood Watch groups, thereôs around 80 but not all are active, some are in limbo.ò

(Interview ID 176, male, 73 years, UK)

This quote provides examples of the wide range of community safety initiatives which have links to NW, and the strong sense of community duty which this volunteer displays. It would be a misconception therefore to view NW activities in the UK in isolation from other community initiatives, as it was a common theme for NW volunteers to be engaged in several other community based activities in addition to NW.

6.3 ACTIVE CITIZENSHIP AND CARING FOR OTHERS

Active citizenship and caring for others is a theme most commonly found in the UK, but is also evident in some of the other countries too. The actual surveillance which individuals or groups then carry out is likely not to have been negotiated and agreed with all of the residents, some of whom will not even be aware that it is happening, when or where it is occurring, or who is carrying it out. The people carrying out the surveillance will probably not have been democratically elected, and in that sense, their actions lack democratic accountability. On

balance, more good than harm will probably come from these forms of óactive citizenshipô in terms of community togetherness and a feeling that something is being done to address the problems which the community is facing. However, the surveillance being undertaken calls into question the democratic right to carry it out; the accountability, accreditation or qualifications of the persons undertaking it (including whether or not any criminal convictions checks have taken place); the potential asymmetrical use of power, and to what extent the local community are kept informed and have some influence over what is happening.

The first quote is an example of what appears to be a self-appointed community ówatcherô who clearly spends large amounts of time watching the daily life activities of the residents where he lives.

> *ñI know at most who lives in the houses. But we have one [guy] in the first house of the street who knows everything. There is nothing he is not aware of. Immediately é when my car window is not completely closed, he comes óyour window is not closedô. It is not unpleasant é he is a nice guy, very bustling, [he] knows everything. I am sure he would respond to something like that é [he] is regarded as pleasant by everybody [in the neighbourhood]. Everybody loves him because he can handle all devices/machines. ôôCome **** something is squealingôô ôôOk, Iôll comeôô. The guy does it without getting paid for it.ò*
>
> (Interview ID 183, male, 79 years, Austria)

The ówatcherô also assists the local community with repairs and advice regarding their domestic appliances, and while it would be harsh to criticise this person for the good role which he performs, as it is a positive account of surveillance, it also demonstrates how the surveillance which he undertakes is not negotiated, and most people will probably not even know it is happening. To that extent the surveillance can be regarded as an asymmetrical use of power in which the ówatchedô have been disempowered, although they will generally be aware that it is occurring, and possibly tolerate its existence.

The second quote is an example of a rural NW community who have lived in the same area for the past 25-30 years. They make sure properties are secure when people are on vacation, and share personal information with each other such as holiday plans and mobile phone numbers:

> *ñIôd say we have a good community here. We are all part of the same generation, we moved to this community of terraced houses 25 ï 30 years ago, we all raised our children here. Although now this turns out to be problematic, we are all old now, no youngsters are living here. But weôve exchanged our mobile phone numbers and we know if someone of our community is on vacation and we can operate the burglar alarm of our neighbours, we have keys to the other apartments we take care of each other. Even the people living in the single-family-houses over the street take care. We, and we are very active in that, notice if somebody is not from here. We warn each other in case there is a stranger coming to our street. We communicate. We share the sweat bath, the pool and we organise evenings where we eat and drink together or where we clean the pool together, we constantly communicate with each other. Now*

as we are all growing old together we are going to the supermarket for the other one if he is sick. It is almost very rural here in this area. Everybody knows everyone. They don't have this kind of atmosphere in the city centre. And the neighbourhood watch scheme is a good thing, we get notifications by e-mail from the head of the scheme if something has happened somewhere. Not only burglaries, even cases of girls being raped are reported to the community. But that existed even before the scheme became active. As I moved into this place, 30 years ago, they've put flyers on trees or the garden fence "Attention, there was a burglary (attempt) in this street!"

(Interview ID 275, female, 72 years, Austria)

This NW group perform a monitoring role over movements in their community and look out for older members of the community who may require additional help. They also socialise with each other, and a very strong sense of caring is evident. Perhaps due to the length of time that some of the members have known each other, and the strong social ties which have developed, this form of NW provides a very good example of how traditional concerns of NW such as crime and fear of crime, have possibly become less important than the fundamental societal and caring needs of the community.

The final quote is both a descriptive and a normative account of how disillusionment with politicians and the police, led this NW volunteer to come to the opinion that you are better off taking control of your own NW activities, and independently of other agencies:

"A key moment for me was the self-experience of becoming a victim and not knowing what else is happening in my close neighbourhood. When our organisation became active I once invited a high ranked police officer to one of our meetings and confronted him with the fact that the police are not doing anything at all when they say they are running a programme on community policing. That community policing or community safety approach already existed for 5 years when we started with our organisation. But there was nothing besides platitudes from politicians. They've initiated a meeting of citizens, police and politicians. That can't be true I thought to myself, the community policing initiative was already dead at this point in time. Ok, so they've invited citizens to this meeting, and you won't believe it but I was the only citizen who has attended this meeting, the rest were policemen and politicians talking to each other. That was a priceless exercise and I don't talk to politicians. No matter which side you choose (he refers to the strong dichotomy between social democrats and conservatives in Austria) they will always say the opposite. So I started to drive around in my car and passed flyers to people on a street level, that is how it all has started with our neighbourhood watch scheme."

(Interview ID years, male, 67 years, Austria)

This quote is representative of most of the countries from which the surveys took place, in that NW tends to be 'bottom-up' originating from within communities and not having been subject to 'top-down' initiatives or directives from politicians, governments or the police. In this sense, the NW scheme is 'owned' by the members (and possibly the community) who set the rules for its operation and control all aspects of it.

6.4 CITIZENS WATCHING CITIZENS (CWC)

CWC can be conducted in both overt and covert situations. Conducted covertly, the surveilled may not be aware that surveillance is happening and therefore cannot express an opinion about it or react to it, although it is a situation in which someone (or some group) is exerting power over them and they are powerless to respond. A large percentage of NW activities will fall into the category of covert surveillance as described above in which the surveilled are unaware that it is happening and are therefore disempowered. Conducted overtly, citizens may be aware that they are being watched, and this may create alternative responses of uneasiness as shown in the first example provided below; both support for it and anger, as given in the second example, and resigned contentment or tolerance to it as provided in the third example.

The first quote is an example of surveillance (in this case CCTV) being installed for a specific purpose, but due to the indiscriminate nature of its lens, the interviewee felt uncomfortable with other people viewing what he was discarding in the rubbish bin, and a lawyer living in the same apartment block also objected to its presence:

> ***ñ****They installed a camera in our house, in a room next to the house with the rubbish bins. They did it after a Shisha Bar was opened in the basement and our caretaker suspected them of leaving their trash in our bins. But a lawyer living in our house objected to it. The idea was that people should call the caretaker when they saw "suspicious" trash, but it didn't work. I also did not feel comfortable, because anybody could see what I was throwing away. Anyway the situation did not improve in the end.****ò***
>
> (Interview ID 56, male, 38 years, Germany)

This quote demonstrates the ubiquity of surveillance, and how people cannot escape it due to its indiscriminating nature and although initially probably accepting of the need for its introduction, citizens may eventually feel the pervasiveness of it in their lives and ultimately reject it.

The second story provides information on a very direct and (usually) visible form of CWC, through Community Speedwatch. This method of traffic speed control involves trained volunteers pointing a speed gun at vehicles driving through an area known in the past for speeding, and has generated mixed responses from the general public, both positive and negative:

> ***ñ****The local Police force where I live has a community engagement model, and they have prioritised road safety and speeding. A pilot project (Community Speedwatch) was trialled in a neighbouring town, which has been running for 14 months, and a new Community Speedwatch project has now started in my town. We are provided with dates and times by the Police, and a team of 3 (volunteers) go into the designated areas, the Police will risk assess it first, we will use the speed gun, and for those who have exceeded the levels we take their details (i.e. car registration number), and pass them to the Police. The Police will then write (a letter) to the owner advising them that*

they have been caught speeding on this occasion but next time they could be charged (with a criminal offence). The Police provide training, and there has been a reduction in the number of speeders and in complaints (by the public about speeding). There has been a mixed reaction ï some people have asked what we are doing, and others have congratulated us saying it is a worthwhile cause, and some give us rude gestures shouting óget a lifeô and then accelerate away. It is definitely worthwhile, as less and less people are speeding ï I passed a location yesterday and the Police had the speed gun. There was a 12 month review in April past, which was positive.ò

(Interview ID 218, male, 27 years, UK)

This example is unusual in that it is an open form of direct surveillance of CWC, and therefore almost invites a response from the public being watched, with some people having supported the initiative, while others have shouted derogatory remarks as they drove past. It is unlikely that the speeding motorists would have shouted the same unkind remarks to police officers if they had been carrying out these duties instead of the volunteers. The example does provide a participatory form of overt surveillance in which the motoring public can moderate their driving behaviour (and speed) as a response to the actions of fellow citizens.

The final quote is a story, which although emanating from Austria could have come from any of the countries from which the interviews were conducted. It describes the role (probably mostly unobserved) of the caretaker who conscientiously and covertly watches the movements in and out of the residences, which he/she looks after:

ñWe have very good caretaker in our residence, who carefully watches our house. So if someone takes out the trash, you will be observed. But I think itôs kind of protective and itôs nice. I have a bike in Vienna, but not enough space in the bicycle rack, so I just left it somewhere. I forget to lock it and three hours later the caretaker ringed, and noticed that I STILL hadnôt locked my bike. So our residence is watched out for. (laughs). And I think itôs nice, it doesnôt bother me because itôs this rural feeling.ò

(Interview ID 502, female, 21 years, Austria)

The surveillance being undertaken although non-negotiated and covert, is accepted with good humour and a situation exists of what could be best described as ó resigned contentment.ô The residents however no longer have the right to remain anonymous, but on balance probably most of them are content with this arrangement and tolerate the surveillance.

6.5 FEAR OF CRIME AND PROPERTY PROTECTION

This section addresses some of the fundamental issues, which exist about both actual crime and the fear of crime, and what the response is of citizens to either condition. In the UK, research has shown 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 for example in one of the least deprived areas of

England.[267] However, living in an area which experiences higher incidences of crime does not mean that there is greater likelihood of NW schemes being established, as in fact higher numbers of NW schemes are found in more affluent areas which also experience lower crime rates, than in more deprived areas which experience higher crime rates.[268] This was also identified in the British Crime Survey in 2006/07: *óIn general, the characteristics associated with lower levels of (NW) membership were those related to having a higher risk of crime.ò*[269] Bennett, in a previous study also came to this conclusion.[270] The relationship, in the other countries examined, between NW start-ups and the relative affluence of areas and their crime rates, is thought to be unexplored.

The first quote is initially a descriptive story of someone who has experienced an attempted burglary, but then provides a normative account of her feelings towards the apparent futility of deploying technological measures to prevent such occurrences:

> *ñYes, I talk about crime with my neighbours, as all my neighbours have been victims of burglaries, and I have been victim of an attempted burglary, but they succeeded only in breaking a window, but I came back home after just 15 minutesé I was so angryé I immediately asked my daughter to close the gate and I went out, as I saw two guys passing by I simply shouted that the police were coming and they didnôt reply to me obviouslyé When something strange occurs in our street, we are used to phoning each other to keep ourselves informed about the potential danger. We do not talk about how to prevent crime, since the majority of my neighbours are old people who are fearful (or live in fear): they lock the door and take other precautionsé maybe I will feel the same when I am old. I think that technical or technological measures are useless, my neighbour (a 75 year old lady who has a husband with health problems) who has been victim of burglaries three times, has bars to her windows but I think they are useless systems of preventioné nobody has installed alarm systems.ò*
>
> (Interview ID 208, female, 62 years, Italy)

It could be argued that the interviewee has a positive outlook to informing her neighbours about strange occurrences in her street to warn of potential danger, but is then at best ambivalent or at worst dismissive of the usefulness of deploying security technologies to prevent crime.

The second story demonstrates the self-empowerment and resilience of a small community living in an apartment block to fight back against a series of burglaries:

---

[267] 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.
[268] Topping, John, Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake, 2012.
[269] 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.
[270] Bennett, Trevor, Themes and variations in neighbourhood watch, Crime, Policing and Place: Essays in Environmental Criminology, Routledge, 1992, pp.172-186.

ñI only registered with neighbourhood watch last year. I have lived at my address for 35 years and it is a quiet area. It is mostly 2/3 bedroom flats in tenement blocks, which makes them suitable for letting. However, the flats in my area started to be targeted by house-breakers, and over a short period there were 10 break-ins or attempted break-ins. I went to the Police for advice and help, and they said they would send a Community Police Officer to give advice. Despite waiting, nobody came, so I went back to the police who then told me that Community Police were disbanded and suggested that I contact neighbourhood watch. I was not happy getting the run-around. Another neighbour was then burgled, so I went to a neighbourhood watch meeting in an area close by. The Police eventually came to see me and attended for 2 hours and they increased their patrols. Most people in our street were much more aware, and I was encouraged to buy an intruder alarm, but the police did admit this would just be moving the problem on elsewhere. My neighbours and I fitted a new metal plate to the communal entrance door to the flats. I also fitted new glass storm doors. The burglars had been watching for the postman arriving, and then gaining access to the communal stairwell by going in behind him, so we deactivated the service button which means the postman has to wait outside for someone to come and take their mail. This 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. I am not wildly happy with the Police ï they clearly did not want to be bothered, but a very good Police officer did speak at the other neighbourhood watch group meeting which I attended.ò

(Interview ID 441, female, 64 years, UK)

An additional social benefit arising from the formation of this NW group has been the fact that the residents now share holiday information and are more sociable with each other than had been the case previously. This example of CWC also shows how having given up on trying to enlist the help of the police to deal with the burglaries, led to the NW group taking decisive action themselves and feeling empowered through the process.

The final quote in this section is a normative account of how the (apparently unsubstantiated) fear of crime and lack of faith in the ability of the police to inform residents about criminal acts, has obscured the intervieweeôs objectivity in being able to rationalise his feelings between fear of crime based on actual occurrences, and perceived threats of crime:

ñIn the year 2005/2006 there was a burglary and theft from the dwelling of one of my daughters, and someone has also broken into my own house. I live on the outskirts of the city and I thought I live in paradise. I always had the feeling that everything in my neighbourhood is peaceful and fine, but then Iôve started to talk about such things with my neighbours. One told me that there were two burglaries just a few weeks ago down the street where we are living. Then I came to the conclusion, that it isnôt that peaceful at all here, crime is happening all the time and everywhere, but nobody knows about it and people donôt inform each other about these issues. The police do not inform neighbours about crimes and have not done so for decades when it would

have been their duty. Even the police spokesman said on national TV that they donôt have the time to do that.ò

(Interview ID 334, male, 67 years, Austria)

This example, along with others from citizens similarly in the older personsô category, perhaps demonstrates an increasing fear of crime as one becomes older and a view of society as being far worse and more unsafe than in reality it actually is. The interviewee regarded living in their neighbourhood some years previously as idyllic, and now there is disillusionment with the police over their ability to maintain law and order.

6.6 RIGHT TO ANONYMITY

The right to remain anonymous, and to be forgotten, is closely aligned with the fundamental right to personal privacy, and the almost impossible task of keeping oneôs personal details, daily movements, conversations, transactions and interactions private.[271] As shown in many of the examples provided, the ówatchedô have had this right removed through the various forms of non-negotiated NW surveillance undertaken, with the requirements of the ówatchersô superimposed on the ówatchedô, and while some might accept this as a necessary part of living in a shared apartment block or a close-knit community, others clearly view it as an infringement of their personal rights and have taken decisive action to attempt to reclaim their right to anonymity which included relocating from suburbs or small towns to the city where they feel that it is easier not to be noticed and to become anonymous. The establishment of the right to be anonymous may have more resonance in those countries, which had totalitarian pasts.

The first quote provides a story of someone who chose to move from the suburbs to the city, where they are enjoying not being subjected to the ubiquitous gaze of surveillance and gossip from neighbours, which had formerly been the case:

ñI am living here for 4 months and don't know anybody, but I don't miss a thing. That's why I live in the city, because being anonymous is possible. I've grown up in a small suburb town in Bavaria, there it was different, the gossip and all, I hate it. Neighbourhood Watch? I know that from ALF, the TV-show. In Munich? Oh please. Nobody lives here against his will, the rents are very high, and you know what you get: sometimes it's a little loud at night, yes. If you don't like that: Leave.ò

(Interview ID 265, female, 31 years, Germany)

This account provides an insight into the thoughts and feelings of someone who had been uncomfortable with the omnipresence of surveillance while living within her local suburban community, and had felt powerless to change that situation. To remedy the situation she had

[271] Szekely, Ivan, *ó The Role of Remembering and Forgetting in a World of Increasing Surveillance, in the Context of Post-Communist Societiesô*, in Living in Surveillance Societies: The Ghosts of Surveillance, Proceedings of LiSS Conference 2, Webster, C. William R., Doina Balahur; Nils Zurawski; Kees Boersma; Bence Sagvari; Christel Backman and Charles Leleux (eds.) University Press óAlexandru Ioan Cuzaô, Iasi, Romania, 2011, pp. 32-36.

chosen to move to the city where she could exercise her right to be anonymous, which she was clearly at ease with.

The final quote is a normative account which provides another example of someone who has consciously made a decision to live anonymously in the city, but who is very well informed about the benefits and disadvantages of sharing part of your life with neighbours and the resultant effects which this can have in a surveillance sense:

> *ñWell I am someone not so engaged with my neighbours. And then there is ambivalence. On the one side you can help each other and support others, but that is more for small townsé not for cities. On the other hand there is that normalising effect, they control you. So I am quite happy to live anonymously in a larger city.ò*
>
> (Interview ID 823, male, 25 years, Germany)

This quote refers to the apparent cultural norm of neighbours in small towns helping each other, but the interviewee does not expect that form of mutual support to exist for those living in the city. The interviewee also refers to the ónormalisingô effect of surveillance, and the control, which those undertaking it can then exert. There appears to be inevitability about surveillance taking place in ósmall townsô, which is likely not to have been negotiated and involves a group of neighbours who can exert power in an asymmetrical manner over other members of the community. If anyone is unhappy living with this form of surveillance, then one option appears to be to relocate to the city and to live anonymously.

6.7 MASTER STORIES AND KEY DILEMMAS

The central themes and key dilemmas which have emerged from the cross-country analysis of CWC and NW surveillance include the democratic accountability and governance of NW, and the societal, cultural and historical reasons which lie behind its growth or indeed its relative lack of development.

The first quote is a story from a NW co-ordinator from the UK who lives in an affluent area *(óall detached housesô)* where she admits that there is little crime, however the neighbours have decided to form a NW group, possibly for reasons of mutual support and shared societal values:

> *ñI am neighbourhood watch co-ordinator of a small patch ï 31 houses, and 4 streets in the local area. All detached houses. Moved there in 1988, and was asked if I wanted to join (neighbourhood watch) ï at that time all 31 (households) were members. (I was) then asked to be a street co-ordinator, which I did for several years, then the main co-ordinator was retiring. I believe in the saying ôôif you know your neighbours you will know the strangers amongst youôô and I was keen for a social event for the neighbours to get together. The Annual General Meeting was more of a social get-together but more people attended than normal. There is little crime, but a few bits and pieces. I joined the Safer Neighbourhood Teams and went on to that as a representative from neighbourhood watch ï others had much more problems than our*

area. We keep eyes and ears open for each other, such as letting the street co-ordinator know about holiday plans and keyholder information.ò

(Interview ID 174, female, 64 years, UK)

This story matches the findings of several academic studies in the UK, which found that NW schemes were more likely to be formed in more affluent areas with lower crime rates, rather than in areas, which were less affluent and had higher crime rates. This phenomenon was not found elsewhere in other countries, which formed part of the study group. The residents of this particular community will, in all probability, have similar backgrounds in terms of professional training, income levels and employment, and can therefore identify easily with each other through shared social values. The surveillance undertaken is likely to be covert although neighbours will be aware that it is happening. The phrase *áIf you know your neighbours you will know the strangers amongst youô* has a particular resonance in relation to CWC.

The second quote is a story which although brief, manages to capture a number of the themes which are emerging throughout this contribution, including: democratic accountability, consent, negotiation, discomfiture, privacy and anonymity:

ñIn my house, there is a couple, they know everything about each and everybody and talk about that to everybody. Horrible. And they offered me, when they "heard" that I was going away for some weeks, that they would care for my postbox. And I said no. That's exactly that thing: I have nothing to hide, but I want to decide who is seeing what.ò

(Interview ID 330, female, 34 years, Germany)

The surveillance undertaken in this example has not been negotiated and has not been agreed through obtaining consent of the residents. It is not regulated, and has been imposed on the ócothersô by this ócoupleô who indulge in gossiping with neighbours. It involves the use of power applied asymmetrically over the ócothersô with the interviewee clearly feeling uncomfortable with it, and feels that she has lost some of her privacy and her right to anonymity, and above all her ability to control what is happening.

The final story shows how a NW scheme can be started from the óground upô eventually increase its membership to include around 6,000 registered users, capturing the attention and interest of both local residents and politicians. Crucially though, there is an inherent distrust of politicians clearly evident, and a determination that the scheme should be formed without any influence from public bodies or elected representatives:

ñIt started back in 2007. Back in these days we called our initiative ñHelp burglaryò. We were handing out flyers on a street level to citizens and then we rented a place in a pub for a first meeting. At the day of the meeting the borough council gave me a call. They said that theyôve heard there is a meeting on burglary prevention and security issues in our neighbourhood and the borough mayor wants to join our meeting. Suddenly they realised that this topic could be of interest for them. Back then our topic was indeed a sensation, so Iôve answered, ñyes he can join us but he isnôt giving a

(political) speech to our fellow citizens. I don't want to hear anything from him, he can come, sit down and listen but there will be only citizens talking with the police, no politicians!' Then they asked me how many people will attend, I've guessed something like 30 but at the end the room was packed with 150 people, all addressed by simply handing out flyers on the street. It was the right topic at the right time. At our meeting there was this young man, in his early thirties or something. He said that it's a brilliant idea we are working on and he would like to help us with a website. I was sceptical at the beginning, that would never work I thought. The first website we've launched was only concentrating on issues in our neighbourhood. We had the idea that with the help of this website, citizens could move closer together. At the beginning of our initiative we wrote people's names on paper, their name and so on. Even at our second meeting back in 2007 we had about 150 participants joining us. We offered the option of registering yourself for the neighbourhood watch scheme online at our website later in time. Now everybody can join the neighbourhood watch scheme, people from all across Austria can do that. We have about 6.000 registered users. Yesterday I had 4 new registrations and two incidents were reported to me. That's how it's going.'

(Interview ID 336, male, 67 years, Austria)

This quote from Austria could be representative of any of the countries from where the surveys were undertaken, in that it demonstrates the common desire for NW groups to be independent from the influence of elected representatives, due perhaps to an inherent distrust of politicians and local councils. It also shows the remarkable potential power of a local community to reach out to other communities with their message, in this case enlisting around 6,000 users from across the country. The potential surveillance, which could be undertaken on this scale is far-reaching, although questions do arise over its governance, democratic accountability and legitimacy. The feelings of the largely unsuspecting publics are unknown, but it would appear that they will be unaware of the surveillance, disengaged from it and therefore disempowered.

National comparisons

Since NW has a strong cultural dimension, developing differently in different societies we will briefly compare the situation in the countries involved in this study. Further details with regard to national differences are addressed in the overall country reports at the end of this Deliverable.

Austria

Austria is generally regarded as a very safe country in which to live, and there has been very little public engagement with NW. Any problems of 'insecurity' amongst citizens might be generated from local media hype, as the media often acts in its own self-interests for example if it is a sensational story it will 'sell', but the figures for recorded crimes are extremely low. The authorities might react to public demands for increased video surveillance by installing some cameras. In Linz and Wels there are city watch schemes, however 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. The main stakeholders

include the media, police, activists, political parties, and local communities. The police are not generally supportive of NW or other groups being formed such as citizen patrols or vigilantes, but they still wish to have direct access to citizens. Culturally, there is no tradition of forming NW in Austria as a societal response, and concern for neighbours is not evident as a community or group based response.

Germany

There are very low levels of NW in Germany where there is a strong cultural tradition of citizens complying with the official way of doing things, and anything, which is proposed beyond that is likely to be criticised. The probable response is for individuals to do things unilaterally, and not to organise themselves into groups. Anything, which raises fears stemming from the countryôs totalitarian and right wing past is likely to raise suspicion, with the terms óBlockwartô[272] and óStasiô[273] sometimes being used by the media. The police and the public sometimes combine their arguments to criticise NW over engagement, and in particular whether or not any right wing tendencies might be emerging which serve to motivate people. In general, the Police are not in favour of NW, and politicians rarely vote for it. In northern Germany there is a tradition of the óNachtwandererô[274] who will look after a community in the evening when it is dark, but there is no such tradition in southern Germany, and nor is there a tradition of looking after neighbours as in the case of the UK. The very low levels of NW formation in Germany is due in part to the now culturally embedded and former Prussian historical tradition of people being trained to serve in the armed forces, and complying with authority. There is an underlying and general fear of community groups being formed to do their own thing.[275] However, the óthirdô sector is now growing and it will be interesting to see what the response is of the state to this phenomenon.

Italy

NW in Italy has low levels of implementation, and due to this it has tended to be overlooked both in the public debate and in the academic discourse, and does not feature in national level politics. While in the UK, NW has expanded greatly and has been analysed from different aspects, in Italy NW is more the exception than the ñruleò. There is some evidence of NW in six municipalities of the Lombardy region, which has a dedicated website: ñcontrollo del vicinatoò (neighbourhood watch).[276]

Slovakia

NW in Slovakia is mostly organised as community based responses to problems experienced with the cohabitation between the majority and minority populations, for example the so called ñRoma Citizen Watchesò which are supported by the Ministry of Interior (Office of the Government Plenipotentiary for Roma Communities). The main objectives of these watches is ó*the promotion of community development, the empowerment of local activism, reduction of antisocial acts, the maintenance of public order and the standard of environmental quality in*

[272] Schmiechen-Ackermann, Detlef, Der "Blockwart". Die unteren Parteifunktionäre im nationalsozialistischen Terror-und Überwachungsapparat, Vierteljahrshefte für Zeitgeschichte, *JSTOR*, 2000, pp. 575-602.
[273] Kretschmann, Andrea, Facets of control: Criminal justice regimes in analysis, *Journal of History and Sociology*, 2013, 4, 2.
[274] Enderle, Manfred, *Nachtwanderer: Kriminalroman*, Gmeiner-Verlag, 2009.
[275] Kreissl, Reinhard, *Governing by Numbers*, 2011.
[276] óControllo del vicinatoô (neighbourhood watch): www.controllodelvicinato.com.

*marginalised Roma communities.*ô[277] One of the reasons for the establishment of such óRoma Citizen Watchesô include occasions when members of the Roma community attack members of the majority population and there is an assumption that such ówatchesô can keep order in the community.[278] Another example is where conflict exists between the majority population and the Roma community where there is insufficient police oversight.[279]

Spain

There is not a strong tendency in Spain to form NW as a community response to societal problems. Concern for neighbours is also not evident as a group response. Communities are often polarised either for or against NW, and their participation in either camp tends be active as opposed to passive. NW is continually co-determined by the stakeholders, in whom the media often set the agenda by raising awareness, and the police tend to react to community demands by deploying more resources for example. Creating a context where NW is the solution is not normally politically acceptable, with the state tending to firefight on particular issues. The media plays a strong role in influencing public opinion on NW, while there is some support, equally there is some opposition and resistance to it. NW is not subject to any form of governance and tends to be unregulated.

UK

NW is one of many different forms of community engagement in the UK which uses various surveillance practices, examples of which include community speedwatch, horse watch, rail watch, flood watch, metal watch, church watch, school watch etc. NW membership is high, as shown before, but the actual total number of schemes is thought to be much higher as many schemes have decided not to register with the national co-ordinating bodies. In terms of how NW is co-determined by the different stakeholders, the Scottish Government, Northern Ireland Assembly and UK Governments fund the respective national co-ordinating bodies for Scotland, Northern Ireland and England and Wales. This funding is primarily for staffing costs and offices, with a little remaining for media campaigns or starter packs for new groups. NW is very much a óbottom-upô grass roots activity, which is self-regulating, and generally free from political interference or governance. Close links will commonly be developed with many other groups and the authorities, notably the police, local authorities, and local councillors. At the outset of NW in the UK in the 1980s and 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 downwards to one which is less involved, although in N. Ireland there is a strong police engagement with NW which has been developed from the establishment of a lasting political peace from the late 1990s. In England and Wales there has been a recent change involving the decentralisation of decision making on police matters to 44 area Police and Crime Commissioners, and it remains to be seen how much influence community groups will have on these Commissioners regarding deployment of police resources to communities. The focus of NW activities in the UK has changed in recent years

[277] Cited from the official document Citizen Watches in the areas of Marginalized Roma Communities, http://www.fsr.gov.sk/data/files/ine/obcianske_hliadky_v_podmienkach_vyzvy_FSR.pdf, in Slovak

[278] There is an example of this in small community Huncovce, where they do not have enough police officers and where Roma citizens attacked football players at the stadium. More information in Slovak: http://romovia.sme.sk/c/7147157/v-huncovciach-po-bitke-zavedu-obcianske-hliadky.html

[279] After such an attack, the authorities are planning for a citizen watch in Tisovec: http://romovia.sme.sk/c/7089505/v-tisovci-po-utoku-planuju-obcianske-hliadky.html, in Slovak

from property and crime related issues to a role which involves caring for neighbours, e.g. bogus callers, internet crime, welfare of older people etc. NW is generally unregulated and unaccountable in any formal sense, since members are unelected and not subject to criminal records checks, and some but not all NW schemes will have a constitution. Surveillance and NW has become more 'normalised' in the UK than in other countries, and schemes are commonly formed in response to either real problems such as burglaries, bogus callers, the fear of crime, or simply as a response to a community desire to be ótogetherô where members will have shared backgrounds, social values, home ownership levels, professional training, levels of employment (or former employment), affluence, ethnicity and religion (in the case of N. Ireland). Very importantly, studies have consistently shown that NW in the UK is more likely to be formed in areas of low crime, higher affluence, higher home ownership, low levels of ethnic mix etc. than in more deprived areas which have higher crime statistics and which are less affluent, have greater turnover of tenants, and the residents have poorer life chances.

6.8 CONCLUSION

Haggerty and Samatas describe surveillance and democracy in the following, clearly defined, context:

> ó*Surveillance, when positioned on a normative continuum, tends to sit at the polar opposite of democracy. Democracy rests with the angels, signifying all that is laudable and promising about government. At the other extreme lurks surveillance; a sinister force that threatens personal liberties.*ô[280]

Of course, in the case of NW surveillance this is clearly too simplistic an explanation due to the complex relationship, which it has for citizens trying to come to terms with issues such as democracy, governance, representativeness, citizenship, participation, transparency, privacy, use of power, the right to be anonymous and societal values. Also, human relationships are undoubtedly influenced by the conditions of visible and invisible surveillance found in NW and although these experiences will mostly be positive and reassuring ones, some citizens passively tolerate the gaze of community surveillance either favourably or unfavourably, while others seek to re-establish their right to privacy and anonymity by relocating to the city for example. Establishing or re-establishing the right to anonymity may be more of a concern for citizens in those countries, which experienced totalitarian pasts, and had state-sponsored systems of surveillance installed for the purposes of monitoring the population. However, NW does provide many excellent examples of active citizenship and civic engagement, in which communities enjoy levels of protection, support and self-empowerment which they might not have otherwise experienced, and in those cases the NW volunteers and groups should rightly be recognised for the good service which they perform.

Looking now at the UK, NW has undoubtedly become ónormalisedô in society given the scale and consistently high levels of participation which it has experienced from the 1980s to the

[280] Haggerty, Kevin D. and Minas Samatas, Surveillance and democracy: an unsettled relationship, in *Surveillance and Democracy*, Routledge, 2010, p20.

present day, and it would be inaccurate to say that this was simply because communities were showing resilience and organising themselves due to the lack of support from the police or politicians, although this may have played some part. The reasons for the growth are thought to be more complex. Studies have shown that NW formation in the UK is more prevalent in areas of low crime and greater affluence, and conversely rates of formation are lower in areas of higher crime and lower affluence, and so, for the UK other factors are influencing the growth of NW and other forms of ówatchesô. These include the fear of crime; the need for certain communities to look after each other, particularly vulnerable people, and the need for some citizens who have shared values, backgrounds and professions to form themselves into not only NW groups for mutual support, but in all probability engage in other forms of social activity and active citizenship. In the last few years, there has been a change in the main purposes of NW in the UK from monitoring potential criminal activity and unusual movements in an area, 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 personal internet security. NW in the UK rarely features in the policy discourse at local or national government level, is largely self-regulated, and arguably, there exists a democratic deficit in term of its public accountability.

For countries which have experienced totalitarian and fascist pasts, such as Austria, Germany, Italy and Spain there has been very limited growth of NW and it has not established itself at anywhere near the same levels as seen in the UK. This may be down to various factors such as the lack of a cultural tradition by communities to form groups in response to societal problems, or fears about a possible return to the days of right wing extremism. Opinions by the media, and in some cases the police and politicians, are more likely to enter the public debate, including open opposition to the concept. Where NW has been established, there is commonality with the UK in that it will have been started from óground upô and there is a shared sense of self-determination and eventual self-empowerment when it is achieved. There are examples from those countries with authoritarian pasts, of rejection of any attempt at proposed engagement from police, politicians or public authorities in the process of starting-up NW groups. In common with the UK, NW in those countries tends to be self-regulated and democratically unaccountable.

CWC and NW surveillance are difficult areas for citizens to actively participate in the discourse around them. This is due to the surveillance mostly being carried out covertly, being non-negotiated, unregulated, and lacking any of the usual forms of accountability or governance controls, which a democratically elected body might have. It also has a noticeable imbalance in the power relationship in favour of the ówatchersô who set the rules about why, how, when, where and by whom it takes place, and therefore puts the ówatchedô at a huge disadvantage, but this is also true of many other types of surveillance systems.[281] The central themes and dilemmas which have emerged therefore from the cross-country analysis of CWC and NW surveillance, include but are not restricted to, the democratic accountability and governance of NW, and the societal, cultural and historical reasons which lie behind its growth or its relative lack of development.

[281] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, 2007, p. 23.

7 SUMMARY

Reinhard Kreissl

WP 4 was designed to investigate the surveillance society as a mundane phenomenon, moulding the everyday life of European citizens. We wanted to know how these lay citizens perceives of surveillance and react to the fact of being more or less constantly exposed to different types of surveillance measures. Surveillance and resilience ï two of the key concepts of IRISS ï cannot be considered household words for the layperson. There exists an elaborate academic discourse about these two concepts, but they are not common coinage in everyday language. Although the revelations of Edward Snowden have received ample response in public media discourse, the complex technical, legal, and political ramifications of programs like PRISM are far beyond the grasp of non-experts. While it is important to analyse surveillance and resilience from an expert position (what IRISS did in a number of work packages detailing theoretical issues), it is also important to understand the effects of modern technologies and the surveillance capabilities they entail on ground level in everyday life.

This requires first of all a move out of the ivory tower of academic seminars and libraries. Much of the surveillance studies research consists of either desk research or technological analysis of complex systems, capable to perform all kinds of data gathering and analysis. What remains mostly uncharted is the domain of daily routines of citizens using their mobile phones, electronic banking, online-shopping portals and social media, passing through checks at airports, producing their swipe cards to get access to their offices and walking under the constant gaze of CCTV cameras in public and private spaces. How do citizens perceive of this constant nuisance of identifying, being watched, providing data? And: Is it a nuisance in the first place in their view?

While some studies have investigated public attitudes towards surveillance in a general sense, using opinion polls and questionnaires, very little is known about the way surveillance creeps into the everyday routines of citizens and how they cope with it. From a methodological perspective it makes a difference whether a subject is exposed to a set of general stimuli or questions, choosing from a set of fixed choices to answer or whether s/he produces a complex narrative account of events, actions and experiences in a communicative setting of an interview or a focus group giving respondents the floor to elaborate on what they think is important. In WP 4 we choose this second option to investigate the effects of surveillance from a wider perspective.

In doing this we embarked on an adventurous journey into the real world. Many academics are not used to do this nor are they trained to do this kind of real world empirical research. As a renowned scholar once put it: sociologists are archaeologists by choice. They stick to artefacts instead of going out and observe real life to understand and analyse how the social world works.[282] Opting for such a bottom-up approach, starting with life on ground level, entails a methodological trade-off. While a survey design, using fixed choice questions on a large number of subjects, produces a set of data that can be easily processed using elaborate statistical methods to test pre-defined hypotheses, the ecological validity of the raw data is

[282] Cicourel, Aaron, FN pers. comment.

typically weak. Producing data in a more open, context-sensitive approach, e.g. conducting narrative interviews or doing participant observation yields complex raw data of high ecological validity, but creates intricate problems when it comes to data analysis. Such a qualitative approach to empirical research requires a good theoretical underpinning, linking data, method and analysis in a comprehensive way.

We decided to follow the bottom-up approach for a number of reasons. First, there is a lack of this kind of investigations, secondly, the conceptual toolkit of surveillance studies should be exposed to a rigid empirical testing: do lay citizens perceive of themselves as leaking data containers, are they aware of social sorting procedures, do they perceive of surveillance as a mixed blessing, are they concerned about data-protection and privacy issues, what do they know about the detrimental effects of surveillance and what kind of coping strategies do emerge under the surveillance regime? In addressing these questions we at the same time problematized the relation between lay and expert knowledge about surveillance and resilience. In doing this we addressed one of the key theoretical and methodological issues informing the IRISS project: the different views of surveillance and resilience emerging from different perspectives of detached observer and involved participants.

Involving more than 200 citizens in five European countries in narrative exchanges about their personal, mundane existence as techno-social hybrids produced a complex database of individual stories detailing what it means to live in a surveillance society. The challenge was to analyse and synthesise the individual stories into a larger theoretical framework spanning the geographical area covered in our research. This required a very intense and frequent exchange among the national research teams to develop a shared understanding of the data collected. Pursuing a bottom-up approach always entails an abductive form of reasoning, i.e. a continuous recursive process of combining theory and data driven interpretations.

In WP 4 we used a basic shared actor model to guide this process: individuals were perceived as competent, goal seeking problem solvers acting in an environment (a ñlife worldò) full of information and communication technologies structuring their range of action. We furthermore assumed ï drawing on surveillance studies ï that this produces a number of typified general dilemmas or so-called trade-offs. We addressed citizens as competent actors performing different roles, each creating a specific dilemmatic constellation with regard to surveillance and resilience: Citizens use modern ICT when they act as consumers, when they act as citoyen (i.e. members of the polity), when they seek for information and organize their daily communicative exchange with significant others and friends, and when they are involved in economic processes as members of the work force. For each of these roles we identified a dilemma focussing on the core concept of privacy. In the world of electronic consumerism privacy is traded in for convenience, in the public sphere, the central trade-off, rehearsed in policy debates is between security and privacy. In the realm of personal communication using new social media privacy is traded in for sociality and in workplace settings it is trust that is replaced by surveillance. Finally we also approached citizens who were actively involved in citizen surveillance schemes like neighbourhood watch to find out about their understanding of surveillance.

Taking this broad and comprehensive approach a number of interesting findings can be synthesized:
Surveillance and resilience can be studied in a wide array of different settings. Focussing the critical debate on surveillance in a law enforcement end security context leaves out important domains like electronic commerce or socialising practices using electronic platforms like Facebook.
Citizens perceive of the transformation they are undergoing as techno-social hybrids, although they do not necessarily use the vocabulary of surveillance and resilience to talk about their coping strategies.

A number of routine activities in the everyday life of European citizens have undergone dramatic changes due to the emergence of new technologies and media like the Internet. These changes are acknowledged in the interviews, but they are not commonly linked to surveillance and control.
When it comes to resilience a number of different reactions can be typified, ranging from surrendering to a situation perceived as unchangeable to active measures of precaution like sharing information selectively or refraining from using new social media.
What makes coping strategies difficult to develop is the peculiar nature of modern surveillance assemblages operating in most cases at an invisible, infrastructural level of data processing. Very often there is no tangible interface for citizens (as a police officer would be the interface of public order) and hence in a number of cases we found a lack of understanding about surveillance effects, sometimes producing extreme interpretations at both ends of the spectrum: trivialising and demonising.

An analysis like the one presented here can be seen as a minor, but nonetheless important contribution to the public societal debate about modern technologies, producing new forms of governance and changing the human condition in many ways: it can help to better understand what it means to live as a techno-social hybrid in a surveillance society and what options emerge to create a resilient society, embracing values like privacy, autonomy and equality, though in a probably new ï electronically mediated ï form.

8 REFERENCES

Note: All references based on online articles from *newspapers* quoted in this report were to be found on the Internet under the URLs provided in the footnotes at the end of 2013. Since those numerous articles are referenced in the footnotes, including the URLs, they are not part of the following bibliography.
This bibliography comprises all other references, e.g. monographs, anthologies, magazine articles etc.

Albrechtslund, Anders. "Online social networking as participatory surveillance" *First Monday* 13.3.2008, http://firstmonday.org/article/view/2142/1949

Anderson, Malcom, Jean Carlo and Apap, Joanna: *Striking a Balance between freedom, security and justice in an enlarged European Union*. Brussels, 2002

Andrejevic, Mark. *iSpy: Surveillance and power in the interactive era*. University of Kansas, 2009.

Ajana, Btihaj, *Governing through biometrics. The Biopolitics of Identity*, Palgrave Macmillan, 2013.

Baghai, Katayoun, Privacy as a Human Right: A Sociological Theoryô, *Sociology* 46, nr. 5 (October 1), (2012): 951ï 965,

Bain, Peter, and Phil Taylor, Entrapped by the ćelectronic panopticonő? Worker resistance in the call centre, *New Technology, Work and Employment*, Wiley Online Library, 2000, 15, 1, pp. 2-18.

Ball, Kirstie, Categorizing the workers, in David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, 2002, pp. 201-224.

Ball, Kirstie, Workplace surveillance: an overview, *Labor History*, Taylor & Francis, 2010, 51, 1, pp. 87-106.

Ball, Kirstie, and David C. Wilson, Power, control and computer-based performance monitoring: repertoires, resistance and subjectivities, *Organization Studies*, Sage Publications, 2000, 21, 3, pp. 539-565.

Bankston, Kevin and Ashkan Soltani, Tiny constables and the cost of surveillance: Making cents out of United States vs. Jones, *The Yale Law Journal online*, 2014. http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones

Bannister, Jon, *Cases of Democratic Resistance in Surveillance Society*, IRISS Consortium Meeting, University of Sheffield, 24-26 June, 2014.

Barabási, Albert-László, and Jennifer Frangos. *Linked: The New Science Of Networks Science Of Networks*. Basic Books, 2002.

Bateson, Gregory, *Mind and nature - a necessary unity*. Cresskill, N.J., Hampton Press, 1979.

Bauman, Zygmunt, *Liquid Modernity*, Cambridge Polity Press, 2000.

BBC News UK 2013, *Six admit planning to bomb English Defence League rally*. http://www.bbc.com/news/uk-22344054, June 8, 2014.

Beaumont, P., The Truth about Twittter, Facebook adn the uprisings in the Arab World. *The Guardian*, 25 February, 2011.

Bellamy, Christine, Perri 6, Charles Raab, Adam P. Warren and Catherine Heeney, Data sharing and personal privacy in contemporary public services: the social dynamics of ethical decision making, *Loughborough University Institutional Repository*, 2005.

Bennett, Colin, ñPrivacy in the political system: perspectives from political science and economicsò, *Privacy and Freedom updated: Social science perspectives on privacy*, Citeseer, 2009.

Bennett, Colin, *Knowing how you vote before you do: micro-targeting, voter surveillance and democratic theory*. Session 9, SNN Conference, Barcelona 2014.

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

Bentham, Jeremy, *Panopticon or the inspection house*, 2, 1, 1991 (1791).

Berglez, Regina and Reinhard Kreissl, Report on security enhancing options that are not based on surveillance technologies, *SurPRISE Deliverable 3.3*, 2013. http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D-3.3-Report-on-security-enhancing-options-that-are-not-based-on-surveillance-technologies_v069.pdf

Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam DI Kramer, Cameron Marlow, Jaime E. Settle and James H. Fowler. "A 61-million-person experiment in social influence and political mobilization." *Nature* 489, no. 7415 (2012): 295-298.

Bourdieu, Pierre, *Acts of Resistance: Against the Tyranny of the Market*, The New Press, New York, 1998.

Boyd, Danah, ñWhy youth (heart) social network sites: The role of networked publics in teenage social lifeò. *MacArthur foundation series on digital learningï Youth, identity, and digital media volume*, 2007,pp 119-142.

Boyd, Danah, Scott Golder and Gilad Lotan, Tweet, tweet, retweet: Conversational aspects of retweeting on twitter. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference, 2010*, pp. 1-10.

Boyd, Dana, Networked Privacy, *Surveillance & Society 10* (3/4), 2012, pp 348 -350.

Brandtzæg, Petter Bae, Marika Lüders and Jan Håvard Skjetne. "Too many Facebook ñfriendsò? Content sharing and sociability versus the need for privacy in social network sites." *Intl. Journal of Humanï Computer Interaction* 26.11-12 (2010): 1006-1030.

Brigenti, Andrea Mubi, *Visibility in Social Theory and Social Research*, Palgrave Macmillan, 2010.

Brown, Sheila, The criminology of hybrids: Rethinking crime and law in technosocial networks, *Theoretical Criminology*, May 2006, 10: pp. 223-244.

Bruno, Farnanda. óSurvaillance and participation on Web 2.0ô in Ă*Routledge Handbook of Surveillance Studiesñ* Ball, K, D. Hagerty and D. Lyon (Eds.), Routledge New York, 2012.

Bryant, Susan, Electronic surveillance in the workplace, *Canadian Journal of Communication*, 1995, 20, 4.

Carr John et al., Hitting the moving target: challenges if creating a dynamic curriculum addressing the ethical dimensions of geospatial data. *Journal of Geography in Higher Education, 2014,* publ. online.

Castells, Manuel, *The rise of the network society*, Blackwell, New York, 1996.

Casico, Jemais, *The rise of the participatory panopticon*, The World Changing, 4 May 2005.

Cassirer, Ernst, *The Myth of the State*, Yale University Press, New Haven, London, 2009 (1946).

Cedrola, Elena, and Sabrina Memmo, ñLoyalty marketing and loyalty cards: a study of the Italian marketñ ,*International Journal of Retail & Distribution Management*, Vol. 38, No. 3, 2010, pp. 205-225.

Coleman, Roy, and Michael McCahill, *Surveillance and Crime*, SAGE Publications Ltd, London, 2011, pp. 69-70.

Coll, Sami, ñConsumption as biopower: Governing bodies with loyalty cardsñ, *Journal of Consumer Culture*, Vol. 13, No. 3, 2013, pp. 201-220.

Correa, Teresa, Amber Willard Hinsley and Homero Gil De Zuniga. "Who interacts on the Web?: The intersection of usersô personality and social media use." *Computers in Human Behaviour* 26.2 (2010): pp. 247-253.

Data Protection Act 1998: www.legislation.gov.uk/ukpga/1998/29/contents
Freedom of Information Act 2000:
http://www.legislation.gov.uk/ukpga/2000/36/contents

Delbridge, Rick and Turnbull, Peter,J., Human Resource Maximation: The Management of Labour under Just-In-Time Manufacturing Systems, in Blyton, Peter, Turnbull Peter, J. (eds.) *Reassessing Human resource Management*, Sage, London, 1992, pp.56-73.

Ditton, Jason, "Crime and the city: Public attitudes towards open-street CCTV in Glasgow", *British Journal of Criminology*, Vol. 40, No. 4, 2000, pp. 692-709.

Ditton, Jason and Stephen Farrall, *The Fear of Crime*, Ashgate/Dartmouth,2000.

Downer, S. ôUp Close and Personalô, *Business Life*, British Airways, May 2014, pp 33-38.

Doyle, A., R. Lippert and D. Lyon, (eds.) *Eyes Everywhere.The Global Growth of Camera Surveillance*, Routledge, New York, 2012.

Durinanova, M., ñ*Cameras cut down on Bratislava city crime*ò, The Slovak Spectator, http://spectator.sme.sk/articles/view/22527/3/

Durkheim, Emile, *The division of labour in society*, Simon and Schuster, New York, 1997 (1893).

Dürrenberger, G. and J. Behringer, *Die Fokusgruppe*, Stuttgart, 1999.

Eltantawy, Nahed, and Julie B. Wiest. "The Arab Spring| Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory." *International Journal of Communication* 5 (2011): 18.

Enderle, Manfred, *Nachtwanderer: Kriminalroman*, Gmeiner-Verlag, 2009.

Ericson, Richard V., and Kevin D. Haggerty, *Policing the Risk*. University of Toronto Press, Toronto, 1997.

European Commission, Digital Agenda Scoreboard 2012, Brussels, 21.06.2013.

European Commission, Digital Agenda Scoreboard 2013, Brussels, 12.06.2013.:
https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DAE%20SCOREBOARD%202013%20-%20SWD%202013%20217%20FINAL.pdf

European Crime Prevention Networks, *Review of Scientifically Evaluated Good Practices for Reducing Feelings of Insecurity or Fear of Crime in EU Member States, European Communities*, 2004.
http://www.eucpn.org/pubdocs/review_reducing_feelings_insecurities_fear_crime_en.pdf

Eurostat, *Crimes recorded by the police*. 08 Jun 2014
http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=crim_gen&lang=en,

Farquhar, Lee Keenan. "*Identity negotiation on Facebook. com*" Unpublished PhD Thesis University of Iowa.

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.

Fonio, C., ñThe silent growth of video surveillance in Italyò, *Information Polity*, Vol. 16, No 2/2011 pp. 379-388: http://iospress.metapress.com/content/d187624350281110/

Foucault, Michel, *Discipline and Punish: The birth of the Prison*, Allen Lane, London, 1977.

Foucault, Michel, The subject and power, *Critical Inquiry*, University of Chicago Press, 1982, pp. 777-795.

Frois, C., *Peripheral Vision. Politics, Technology and Surveillance*, Berghahn Book, Oxford, 2013.

Fussey, P., "New Labour and New Surveillance: Theoretical and Political Ramifications of CCTV Implementation in the UK", *Surveillance and Society* 2, no. 2/3, 2004:pp. 251-269.

Gandy, Jr., Oscar H., *The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries*. Westview Press, Boulder, 1993.

Galdon Clavell, G., ñThe Political Economy of Surveillance in the (wannabe) global cityò *Surveillance & Society*, Vol 8 No.4, 2011, pp. 523-526. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4191/4193

Garfinkel, Harold, A conception of and experiments with ātrustô as a condition of concerted stable actions. In Harvey, J.O. (ed.) *Motivation and social interaction*. Ronald, New York 1963.

Garfinkel, Simon, *Database Nation - The Death of Privacy in the 21st Century*, O'Reilly, Cambridge et al., 2000.

Geertz, Clifford, *The Interpretation of Cultures*. New York: Basic Books, 1973...

Goffman, E. *The Presentation of Self in Everyday Life*. Harmondsworth: Penguin Books. 1987 (1959).

Goldbeck, Jennifer, The curly fry conundrum ï why Social Media ñlikesò say more than you might think. http://tedxesl.files.wordpress.com/2014/05/transcript-jennifer-golbeck1.pdf

Greene, Jeremy A., et al. "Online social networking by patients with diabetes: a qualitative evaluation of communication with Facebook." *Journal of general internal medicine* 26.3 (2011): 287-292.

Greenwald, Glenn, https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/Giddens, Anthony, *The Constitution of Society, Outline of the Theory of Structuration*, Cambridge, Polity Press 1984.

Habermas, Jürgen, *Theorie des kommunikativen Handelns* (Band 1 und 2), Frankfurt, Suhrkamp, 2011.

Haggerty, Kevin D. and S. Ericson, ôThe surveillant assemblageö, *The British Journal of Sociology*, 51, No. 4 2000, pp. 701ï 717.

Haggerty, Kevin D., and Minas Samatas, Surveillance and democracy: an unsettled relationship, in *Surveillance and Democracy*, Routledge, 2010.

Hampson, Ian; Peter Ewer and Meg Smith, Post-Fordism and workplace change: towards a critical research agenda *Journal of Industrial Relations*, Sage Publications, 1994, 36, 2, pp. 231-257.

Hempel, L., and E. Toepfer, *CCTV in Europe. Final report*, Working Paper No.15, Centre for Technology and Society, 2004, http://www.urbaneye.net/results/ue_wp15.pdf

Heymann, Philip B. and Juliette N. Kayyem. *Protecting Liberty in an Age of Terror*. Cambridge, Mass.: MIT Press 2005.

Higgs, Edward, *The Information State in England: The Central Collection of Information on Citizens since 1500*, Palgrave Macmillan, Basingstoke, England, 2004.

Horkheimer, Max and Theodor Adorno, *Dialectic of Enlightenment: Philosophical Fragments*, Stanford University Press, 2002 (1944).

Hummelsheim, Dina, Helmut Hirtenlehner, Jonathan Jackson and Dietrich Oberwittler, ñSocial insecurities and fear of crime: a cross-national study on the impact of welfare state policies on crime-related anxietiesò, *European sociological review*, 27 (3), 2011, pp. 327-345.

Information Polity, ñRevisiting the surveillance camera revolution: issues of governance and public policyò, Vol. 17, no 1, 2012. http://iospress.metapress.com/content/r161232517m7

Kammerer, D., ñPolice use of public video surveillance in Germany from 1956: management of traffic, repression of flows, persuasion of offendersò, *Surveillance & Society*, Vol.6 No.1, 2009, pp. 43-47, http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3403/3366.

Khonder, H.H., Role of the New Media in the Arab Spring, Globalizations. Vol 8 (5), 2011, pp. 675-679.

Kosinski, Michal, David Stillwell and Thore Graepel, "Private traits and attributes are predictable from digital records of human behaviour", *Proceedings of the National Academy of Sciences* 110.15, 2013: pp. 5802-5805.

Kreissl, Reinhard, *Governing by Numbers*, 2011.

Kretschmann, Andrea, Facets of control: Criminal justice regimes in analysis, *Journal of History and Sociology*, 2013, 4, 2.

Lagrange, Randy L.,and Kenneth F. Ferraro, ñAssessing Age and Gender Differences in Perceived Risk and Fear of Crimeò, *Criminology*, vol. 27, 1989, pp. 697ï 720.

Lash, Scott and John Urry, *Economies of signs and space*, Sage Publ. London 1994.

Lenhart, Amanda, et al. "Teens, Kindness and Cruelty on Social Network Sites: How American Teens Navigate the New World of" Digital Citizenship"." *Pew Internet & American Life Project*, 2011.

Leleux, Charles, and William R. Webster, The Sale of ôEditedô Electoral Registers in Scotland: Implications for Citizenship, Privacy and Data Protection, *6th Biennial Conference of the Surveillance Studies Network, Surveillance: Ambiguities and Asymmetries*, Barcelona, Spain, 24-26 April, 2014.

Levesley, T., A. Martin, and G. Britain. *Police Attitudes to and Use of CCTV*, Home Office, 2005.

Lewis, Dan and Greta W. Salem, *Fear of Crime: Incivility and the Production of a Social Problem*. New Brunswick: Transaction Publishers, 1986.

Lewis, Kevin; Marco Gonzalez and Jason Kaufman. "Social selection and peer influence in an online social network." *Proceedings of the National Academy of Sciences* 109, no. 1 2012: pp. 68-72.

Luhmann, Niklas, Risiko und Gefahr, In. *Soziologische Aufklärung, 5*, 2 Auflage, Opladen, Westdeutscher Verlag, 1993, pp. 131 -169.

Lupton, Deborah, *Risk*. Routledge, New York, 1999.

Lyon, David, *The electronic eye: The rise of surveillance society*, University of Minnesota Press, 1994.

Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 1997.

Lyon, David, *Surveillance as social sorting: privacy, risk, and digital discrimination*, Psychology Press, 2003, pp. 13-30.

Lyon, David, "9/11, Synopticon, and Scopophilia: Watching and Being Watched", in Kevin D. Haggerty and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006, pp. 35-54.

Lyon, David, Situating surveillance ï History, Technology, Culture; in: Kees Boersma, Rosamunde van Brakel, Chiara Fonio, Pieter Wagenaar (eds.) *Histories of State Surveillance in Europe and Beyond*, Routledge, 2014, pp. 32-46.

Lyotard, Jean-Francois, *The post-modern condition. A report on knowledge*. Manchester University Press, 1979.

MacCahill, M., *The Surveillance Web: the rise of Visual Surveillance in an English City,* Willan, Collumpton, 2002.

McKinlay, Alan, and Ken Starkey, Managing Foucault: Foucault, management and organization theory, *Foucault, Management and Organization Theory*, 1998, Sage London, 1998, pp. 1-13.

Macnaughton-Smith, Peter, The Second Code. Toward (or Away from) an Empiric Theory of Crime and Delinquency *Journal of Research in Crime and Delinquency* July 1968 vol. 5 no. 2 pp. 189-197.

Marx, Gary, T., A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, Vol. 59, N0 2, 2003, pp. 396-390.

Merton, R. K., and P. L. Kendall, ñThe Focused Interviewò, *American Journal of Sociology,* 1946. 51, pp. 541-557.

Milgram, Stanley, "The small world problem." *Psychology today* 2.1 (1967): 60-67.

Mirrlees-Black, Catriona, Pat Mayhew and Andrew Percry, *The 1996 British Crime Survey. Issue 19/96*, Home Office Statistical Bulletin, Research and Statistics Directorate, London, 1996.

Monahan, Torin, *Surveillance in the Time of Insecurity*, Rutgers University Press, New Jersey, 2010.

Mork Lommel, Heidi, ñTargeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norwayò *Surveillance & Society*, vol. 2 (2/3), 2004 pp. 346-360, http://www.surveillance-and-society.org/articles2(2)/unwanted.pdf

Morozov, Evgeny, *To save everything, click here. The folly of technological solutionism*, Public Affairs, New York, 2013.

Mukherjee, Kamal and Bhattacharya, Ranan, Exploring the Mediating Effect of Organizational Trust Between Organizational Justice Dimensions and Affective Commitment *Management and Labour Studies* February-May 2013 vol. 38 no. 1-2 pp. 63-79.

Murakami Wood, D., and William Webster, ñLiving in Surveillance Societies: the Normalisation of Surveillance in Europe and the Threat of Britainôs Exampleò, *Journal of Contemporary European Research,* Vol.5, No 2 (2009) pp. 259-273. http://www.jcer.net/index.php/jcer/article/view/159/144.

Ney, S. and K. Pichler, *Video surveillance in Austria,* Working Paper No. 7, Interdisciplinary Centre for Comparative Research in the Social Sciences, 2002, http://www.urbaneye.net/results/ue_wp7.pdf

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

Nissenbaum, Helen, "A contextual approach to privacy online", *Daedalus* 140.4 (2011): 32-48.

Nietzsche, Friedrich; *Thus spoke Zarathustra (1.11: The New Idol),* Cambridge University Press, 2008 (1883).

Norris, C., and G. Armstrong, *The Maximum Surveillance Society: The Rise of CCTV,* Berg, Oxford, 1999.

Norris, C., *A review of the increased use of CCTV and video-surveillance for crime prevention purposes in Europe***ò** Civil Liberties, Justice and Home Affairs, April 2009, p.10 http://www.statewatch.org/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf

Norris, C., ñThereôs no Success like Failure and Failureôs no Success at all: Some critical reflections on understanding the global growth of CCTV surveillanceò in Doyle, Aaron, Randy Lippert and David Lyon (eds.), *Eyes Everywhere. The Global Growth of Camera Surveillance,* Routledge, New York, 2012, pp. 23-45.

Pariser, Eli, *The filter bubble. What the internet is hiding from you,* Penguin, New York, 2012.

Pollet, Thomas V., Sam GB Roberts and Robin IM Dunbar. "Use of social network sites and instant messaging does not lead to increased offline social network size, or to emotionally closer relationships with offline network members." *Cyberpsychology, Behaviour, and Social Networking* 14, no. 4 (2011): 253-258.

Power, Michael, *The Audit Society,* Oxford University Press, 1997.

Preece, Jenny, "Etiquette online: from nice to necessary", *Communications of the ACM* 47.4. 2004: pp. 56-61.

Pridmore, J., ñReflexive marketing: the cultural circuit of loyalty programsñ, *Identity in the Information Society (IDIS),* No. 3, 2010, pp. 565-581.

Rose, Nicolas and C. Novas, *Biological citizenship*. Blackwell Publishing, 2004.

Rosen, Christine. "Virtual friendship and the new narcissism", *The New Atlantis: A Journal of Technology and Society* 17.2 (2007): 15-31.

Rabinow, P., Artificiality and enlightenment: from sociobiology to biosociality, *Essays on the anthropology of reason,* Princeton University Press, NJ, 1996.

Rummelhart, David, Notes on a schema for stories, In: Daniel Bobrow and Allan Collins, *Representation and Understanding, Studies in cognitive science,* Berkeley, University of California, 1975, pp. 211-236.

Schmiechen-Ackermann, Detlef, Der "Blockwart". Die unteren Parteifunktionäre im nationalsozialistischen Terror-und Überwachungsapparat, Vierteljahreshefte für Zeitgeschichte, *JSTOR*, 2000, pp. 575-602.

Schütz, Alfred, *The Phenonemology of the Social World*. Northwestern University Press, Evanston IL,1967.

Schwartz, B., ñThe social psychology of privacyò, *American Journal of Sociology*, 1968, 73, pp. 41ï 52.

Sewell, Graham, and James R. Barker, ñNeither good, nor bad, but dangerous: Surveillance as an ethical paradoxò, *Ethics and Information Technology*, Springer, 2001, 3, 3, pp.181-194.

Sewell, G., and James R. Barker, ñCoercion versus care: Using irony to make sense of organizational surveillanceò, *Academy of Management Review*, 2006, *31*(4), pp. 934-961.

Sin, Sei-Ching Joanna, and Kyung-Sun Kim, "International students' everyday life information seeking: The informational value of social networking sites." *Library & Information Science Research* 35.2 (2013): 107-116.

Sofsky, Wolfgang , *Das Prinzip Sicherheit*. Frankfurt am Main: S. Fischer Verlag, 2005.

Solove, Daniel J.,*Understanding Privacy*, Harvard University Press 2008.

Spittler, Gerd, Streitregelung im Schatten des Leviathan : Eine Darstellung und Kritik rechtsethnologischer Untersuchungen. *Zeitschrift für Rechtssoziologie* Jg. 1 (1980), H. 1, S. 4-32.

Stallwood, O., ñGame to destroy CCTV cameras: vandalism or valid protest?ò, *The Guardian*, 25.01.2013. Accessed on 22.04.14. http://www.theguardian.com/theguardian/shortcuts/2013/jan/25/game-destroy-cctv-cameras-berlin

Steyaert, S., and H. Lisoir (eds.), *Participatory Methods Toolkit ï A practitionerôs manual*, Brussels: King Baudouin Foundation and the Flemish Institute for Science and Technology Assessment (viWTA) 2005.

Suau, Cristian, and Margarita Munar Bauzá, ñThe mall in the online shopping eraò, Unpublished Paper, presented at the *4th International Conference of the International Forum on Urbanism (IFoU)*, 2009.

Surveillance & Society: ñThe Politics of CCTV in Europe and Beyondò Vol. 2, No 2/3, (2004): http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/CCTV

Surveillance & Society: ñRevisiting Video Surveillanceò Vol. 6, No 1, 2009, http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Relaunch. Accessed on 07/06/14

Szekely, Ivan, ñThe Role of Remembering and Forgetting in a World of Increasing Surveillance, in the Context of Post-Communist Societiesò, *in Living in Surveillance Societies: The Ghosts of Surveillance*, Proceedings of LiSS Conference 2, Webster, C. William R., Doina Balahur; Nils Zurawski; Kees Boersma; Bence Sagvari; Christel Backman and Charles Leleux (eds.) University Press óAlexandru Ioan Cuzaô, Iasi, Romania, 2011, pp. 32-36.

Thompson, Edward P., The Moral Economy of the English Crowd in the 18th Century. *Past & Present*, 50, pp. 76-136, 1971.

Topping, John, *Northern Ireland Neighbourhood Watch: Participatory Mapping and Socio Demographic Uptake*, 2012.
Trottier, Daniel, *Social media as surveillance* Farnham: Ashgate, 2012.
Trottier, Daniel, and David Lyon. "Key features of social media surveillance" In, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media.* Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.) Routledge. New York, 2012, pp. 89- 105**.**
United Kingdom: Human Rights Act 1998: http://www.legislation.gov.uk/ukpga/1998/42/contents
United Kingdom: Regulation of Investigatory Powers Act 2000:http://www.legislation.gov.uk/ukpga/2000/23/contents
United States: Supreme Court of the United States: Riley versus California, 2013. http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf
Vanderveen, Gabry, *Interpreting Fear, Crime, Risk, and Unsafety: Conceptualisation and Measurement*. Boom Juridische Uitgevers 2006.
Verschueren; Paul, From Virtual to everyday life, In: Jan Servaes & Nico Carpentier (ed.), *Towards a Sustainable Information Society,* Intellect, Bristol, UK Portland, OR, USA, 2005, pp.169- 184.
Waldby, C., *The visible Human Project: informatics bodies and posthuman medicine,* London; New York, Routledge, 2000.
Weber, Max, *Economy and society: An outline of interpretive sociology,* University of California Press, 1978.
Webster, William, ñThe Diffusion, Regulation and Governance of Closed-Circuit Television in the UKò, *Surveillance & Society,* Vol.2 (2/3) 2002. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3376/3339
Webster, William, ñCCTV Policy in the UK: Reconsidering the Evidence Baseò *Surveillance & Society,* Vol. 6, No 1(2009) pp. 10-22. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3400/3363
Webster, William, ñPublic Administration as Surveillanceò, in Kirstie Ball, Kevin D. Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, London, 2012, pp. 313-320.
Wigorts Yngvesson, Susanne, The Boss as Big Brother: Moral Aspects of Workplace Surveillance, in Gudrun Vande Walle; Evelien Van den Herrewegen and Nils Zurawski, ñLocal practice and global data. Loyalty cards, social practices and consumer surveillanceñ, *Sociological Quarterly*, Vol. 52, No. 3, Fall 2011, pp. 509-527.
Zhao, Shanyang, Sherri Gasmuck and Jason Martin, Identity construction on Facebook: Digital empowerment in anchored relationships, In: *Computers in Human Behavior,* Vol. 24, Is. 5, 2008, pp-1816-1836.
Zurawski, Nils (eds.), *Crime, security and surveillance: effects for the surveillant and the surveilled,* Eleven International Publishing, 2012, pp. 193-207.

9 ANNEXES

9.1 ANNEX I – COUNTRY REPORTS

Alexander Neumann; Alessia Ceresa, Daniel Fischer, Chiara Fonio, Erik Láštic, Charles Leleux Keith Spiller, Nils Zurawski

Part of the research strategy for this study was to draft country reports along the following research questions to gain a better understanding for national differences that were assumed before we conducted the analysis of the material:

9.1.1 Implementation of the EU data retention directive (2006/24 EC)

Guiding question: How was the EU data retention directive (2006/24 EC) implemented in your country? Were there any public protests, debates?

Results for the UK

The UK is relying on the Data Protection Act rather than the EU data retention directive to guarantee compliance;[283] as a result there appears to be little debate or reaction to the directive by the UK media and public. Instead much debate has focused on the Draft Data Communications Bill, which in effect supersedes much of the authority of the directive. The Draft Bill has received the sobriquet of the ósnooperôs Charterô due to the invasive privileges the Bill could afford to crime enforcement. In brief the Bill proposes;

- Internet service providers having to store for a year all details of online communication in the UK – such as the time, duration, originator and recipient of a communication and the location of the device from which it was made.
- They would also be having to store for the first time all Britons' web browsing history and details of messages sent on social media, webmail, voice calls over the internet and gaming, in addition to emails and phone calls
- Police not having to seek permission to access details of these communications, if investigating a crime
- Police having to get a warrant from the home secretary to be able to see the actual content of any messages
- Four bodies having access to data: the police, the Serious and Organised Crime Agency, the intelligence agencies and HM Revenue and Customs [284]

The Draft Data Communications Bill has faced much vociferous criticism; particularly from UK human rights groups. 285 Liberty (see Section 3.5), for example, has published a sizeable submission to the Joint Committee (a governmental board comprising of representatives of both houses of the UK parliament. Their role is to examine proposed Acts, Bills and Laws). 286 Liberty highlight the potential dangers of outsourcing the monitoring of citizens to, for example, telecommunication providers which they attest effectively asks the nation to monitor the nation. Other criticisms raised have called for greater clarity on the application of the Bill and how and where the huge amount of data captured will be stored and how this data may be analysed or reviewed in the future.

[283] See http://www.computing.co.uk/ctg/news/2075377/watchdog-slams-eu-retention-directive
[284] Source and See, http://www.bbc.co.uk/news/uk-politics-20676284
[285] See http://www.bbc.co.uk/news/technology-18439226
[286] See http://www.liberty-human-rights.org.uk/pdfs/policy12/liberty-submission-to-the-draft-communications-data-bill-committee-aug-2012-.pdf).

Results for Italy

The Directive of the European Union 2006/24/EC[287] on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of the public communication networks has been implemented in Italy with the D. L.gs 30 May 2008 n.109.

In light of the legal modifications in this context, the DPA updated the General Provision on 17th January 2008[288], which represents the complementary legal framework about ñdata retentionò in the electronic and telecommunication context (mobile telecommunication companies, e-commerce, etc.) in order to implement the art. 132 of D. L.gs 30 June 2003 n. 196[289], the s.c. Data Protection Code, enforced on 24 January 2004.

Therefore, according to the Italian Data Protection law, the data retention rules allow telephone/mobile companies to store certain data related to phone calls, including SMS messages, made/received by their customers for 24 months. In detail, the data retained includes the number of the phone that is making the call and the name and address of the customer, as well as the phone company which provided the phone number, the dialled number/s, the date and hour of the start-end of the phone call, the codes of the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of both the maker and the receiver of the phone call and finally the data which enables the geolocalisation of the call (caller ID). The period of data retention is reduced to 30 days in cases of phone calls without reply. Furthermore, the data retention for SMS is related to the sender, receiver, place and time of the message, even when the SMS has been sent or received via the Internet: VoIP, e.g. ñVoice over IPò, this is the case, for instance, when using Skype, Viber or Whatsup online services. It is evident that the typology of stored data refers to the technical data of the phone call or SMS but never to the content of the (verbal or written) communications, according to the Italian constitutional principle of the ñcommunications privacy right, whatever communication method is usedò[290]. Infringement of this constitutional principle is allowed only under approval of a judicial authority order (public prosecutor, magistrate or lawyerôs request) for (personal and/or public) security reasons (e.g. terrorism or other violent crimes)[291].

The other focus of this legislation refers to the data retention in cases of electronic communications. In this case, the data retention legislation refers only to the data related to the origin of the communication, not to the destination. In detail, the DPA defined that ñ*the information collection on the web sites visited by the customers, even when there is a specific URL or a generic IP address of destination*ò[292] is forbidden. The only exception is to identify the destination of the information as already mentioned in cases of SMS or e-mail sent via the Internet (VoIP, i.e. ñVoice over IPò), as they are the equivalent to a phone call. Therefore, the data can be stored for 12 months and the data retention refers to the IP address, the customer name and address, the typology of service and the access line (the number of the line if ñdial upò, number of DSL or other). Also, in this case, the information about the content of the communication is excluded for the same constitutional right and the exception for communication content retention is the judicial authority order[293], as mentioned in the data retention rules in cases of phone-call communications.

The introduction of the European Directive 2006/24/EC concerning the ñdata retentionò issue within the context of electronic communications services or public communications networks has not been the object of diffused public protests or debates involving the citizens at a national level.

---

[287] European Parliament and the Council, Directive 2006/24/EC of 15.03.2006 on the retention of data generated or processed in connection with the provision of public available electronic communications services or of public communication networks and amending Directive 2002/58/EC, in OJ L 105/54-63, 13.04 2006

[288] D.L.gs 30 May 2008 n. 109, in G.U. 5 February 2008 n. 30

[289] D.L.gs 30 June 2003 n. 196, in G.U. 29 July 2003 n. 174 ï Supplemento Ordinario n. 123

[290] Art 15 Italian Republic Constitution

[291] Minozzi Marzia, ñData retention ï Gli operatori telefonici non conservano i contenuti delle chiamate e degli SMSò, in *Sicurezza e Giustizia*, No. IV/MMXI, 2011, pp. 24-25

[292] DPAôs provision of the 10 January 2008, www.garnteprivacy.it

[293] Minozzi Marzia, ñData retention ï Gli operatori telefonici non conservano i contenuti delle chiamate e degli SMSò, in *Sicurezza e Giustizia*, No. IV/MMXI, 2011, pp. 24-25

In fact, the reaction against the European Directive 2006/24/EC has been expressed much more at a European level through the EDRi (European Digital Rights) organisation report[294]. The support for the European protest in Italy has been represented by Netcomm (one of the three main European e-commerce associations)[295] and in particular by the company President, Roberto Liscio, who officially declared to the Italian newspaper, *Corriere della Sera*, that ñ[the enforcement of the Directive 2006/24/EC, especially concerning the aspect of e-commerce] *would increase the costs of transportation, up to 10 billion Euros*. [...] *in fact we are going to increase the transportation expenses from 5,7 billion Euros to 15,6 billion Euros* [...] *and many small-medium companies would risk closing their activities, and many ósstart-upsô wouldnôt even be born at a time where there is the necessity to develop the strength and vitality of managers, both in Italy and Europe, to support the economy and overcome the crises we are currently experiencing* [...]ò[296].

An answer to Netcomm was given by the General Secretary of Adiconsum (a consumer association supported by the CISL labour union), Pietro Giordano, who was in favour of the Directive 2006/24/EC: ñ*the Directive will produce negative effects only against those who operate improperly in the market* [...]ò[297]. Therefore any protest remained at a European level because, in Italy, there havenôt been demonstrations or public protest events involving the citizens or associations/organisations active in the data protection and/or privacy context.

On the other hand, the implementation of D. L.gs n. 109/2008 (on the base of the EU Directive 2006/24/EC) has concretely demonstrated its effectiveness through a recent inspection of the Fiscal Police-Special Privacy Nucleus (Guardia di Finanza-Nucleo Speciale Privacy in Rome), supported by the Italian DPA, of 11 mobile and provider companies to check whether these companies are using and storing personal data according to the law and procedures in line with the privacy rights, as well as the data retention directive.

The Fiscal Police, in fact, found that 9 companies out of a sample of 11, infringed the law of ñdata retentionò and the privacy rights of the mobile companies and providers[298]. Therefore, the result of this inspection demonstrated that, *a priori*, there is a clear lack of knowledge and awareness by the mobile companies and providers of the legal framework on this issue. In fact, one of the main scopes of this police inspection was precisely to develop and spread the implicit ñmessageò about the importance of the legal management of sensitive data, according to the data retention and privacy related to the new technological channels of communication, also in light of the wide diffusion in the market of the brand new *smartphone* and *tablet* technologies in this field, i.e. a message about the necessity of protecting the consumersô personal data and privacy[299].

The Fiscal Police discovered several law infringements regarding data retention and privacy, i.e. the violation of the retention period to store the customersô data beyond the legal requirement (24 months for phone calls and SMS; 12 months for electronic communications, i.e. Internet services) and the violation of the principle of deleting the collected data at the end of the storage period; the lack of minimum standard security measures that should be adopted by the mobile companies and providers; the infringement of the DPAôs provision about the adoption of biometric measures, by which the data to be stored and those that should be deleted can be recognised [300].

---

[294] European Digital Rights, ñShadow evaluation report on the Data Retention Directive (2006/24/EC)ò, 17 April 2011,
[295] The three main e-commerce associations in EU are Fevad (France); Netcomm (Italy) and Imrg (UK)
[296] http://lareteingabbia.net/tag/rete/page/8/
[297] http://lareteingabbia.net/tag/rete/page/8/
[298] D.L.gs 30 May 2008 n. 109, in G.U. 5 February 2008 n. 30 (implementation of the EU Directive 2006/24/EC); DPAôs General Provision of the 17 January 2008
[299] Garante per la protezione dei dati personali, ñPrivacy: operazione ódata retentionô. ispezione della Guardia di Finanza in tutta Italia sul rispetto delle norme per la conservazione dei dati di traffico telefonico e telematicoò, Rome, 6 March 2013, www.garteprivacy.it; Federprivacy, ñPrivacy & Telecomunicazioni: ispezione della Guardia di Finanza in tutta Italiaò, March 2013, http://www.federprivacy.it/news-mobile/805-privacy-a-telecomunicazioni-ispezioni-della-guardia-di-finanza-in-tutta-italia.html
[300] Assodigitale, ñViolazione dei dati personali e della privacy, brutte notizie dallôoperaizione ódata retentionô delle Fiamme gialle: codice violato in 9 casi su 11ò, March 2013, http://www.assodigitale.it/2013/03/06/violazione-dei-dati-personali-e-

At the end of the police inspection at a national level, two cases about the infringement of the data retention law and the violation of the legal period to store sensitive data were reported to the Minister of the Economy, and the DPA were informed about a case of crime against the minimum standard security measures. Consequently, the DPA will define the legal line between privacy and data retention rights within the next few months, on the basis of (private and public) security reasons, especially in cases of data transfer abroad[301].

Results for Austria

As the Austrian government didnôt meet the deadline of the implementation of the Data retention directive (15th March 2009), the European Commission filed a complaint on the 10th July 2010. In order to circumvent the payment of a fine, the directive was finally implemented and became applicable on the 1st April 2012. The delay of the implementation was the consequence of a lack of support for the directive in the national government. Since the beginning of 2007, thus during the timeframe of the implementation, Austria has been governed by a grand coalition, consisting of the Social Democratic Party of Austria (SPÖ) and the Christian democratic and conservative party ï the Austrian Peopleôs Party (ÖVP). Only the ÖVP showed full support and was willing to implement the directive as it is. The SPÖ, in charge of the implementation, raised a lot of concerns, especially regarding data protection and thus postponed the implementation willingly to debate the directive on the European Level. This debate never happened and the SPÖ were forced to implement the directive, but did only the bare minimum, i.e. the storage of communication data during a period of 6 months. The access through a prosecutor is only possible by judicial decision in case of a ósevere offenceô, which is defined as a crime with a minimum sentence of 3 years; concretely listed are 32 types of offences. In case of imminent danger, the police have the possibility to access the data without a judicial decision. Every access has to be reported to a commissioner for legal protection.[302]

On the opposition base, all the political parties were strictly against the Data retention directive, even the Alliance for the Future of Austria (BZÖ), who voted in favour of the directive on the European Level as governing party in 2006. The concerns of the opposition parties were primarily due to the threat of peopleôs privacy and the conflict of the directive with the Art. 8 of the European Convention of Human Rights.

In November 2012, a total of 188 accesses have been reported by the authorities, resulting in 19 solved cases. This reinforced the opposition in their criticism regarding the usefulness of the data retention, as none of the accesses has been triggered by a case of terrorism, which was the main reason for implementing the directive.[303]

The main public debates and protests against the Data retention directive occurred around the 1st April 2012, the time of the implementation in Austria. On the 31st March 2012 throughout Austria, demonstrations were organized, labelled with ófarewell privacyô.[304] Between 500 (according to the police) and 2000 (according to the organizers) people participated solely in Vienna, 9000 people were

---

della-privacy-brutte-notizie-dalloperazione-data-retention-delle-fiamme-gialle-codice-violato-in-9-casi-su-11/; Federprivacy, ñPrivacy & Telecomunicazioni: ispezione della Guardia di Finanza in tutta Italiaò, March 2013, http://www.federprivacy.it/news-mobile/805-privacy-a-telecomunicazioni-ispezioni-della-guardia-di-finanza-in-tutta-italia.html

[301] Garante per la protezione dei dati personali, ñPrivacy: operazione ódata retentionô. ispezione della Guardia di Finanza in tutta Italia sul rispetto delle norme per la conservazione dei dati di traffico telefonico e telematicoò, Rome, 6th March 2013, www.garteprivacy.it; Federprivacy, ñPrivacy & Telecomunicazioni: ispezione della Guardia di Finanza in tutta Italiaò, March 2013, http://www.federprivacy.it/news-mobile/805-privacy-a-telecomunicazioni-ispezioni-della-guardia-di-finanza-in-tutta-italia.html

[302] http://www.akvorrat.at/sites/default/files/VDS_BIMEntwurf2009/BIM-Entwurf_TKG-Novelle_2010.pdf S14

[303] Der Standard 28.11.2012 Vorratsdaten: Bisher 188 Abfragen durch Behörden in Österreich http://derstandard.at/1353207614601/Vorratsdaten-Bisher-188-Abfragen-durch-Behoerden-in-Oesterreich 08.04.2013

[304] https://gegenvds.at/ 08.04.2013

expected by Anonymous Austria.[305] In Linz, a total of 500 participants were recorded at the demonstration.[306] Already in 2011 some minor demonstrations against the data retention were organized in Graz and Linz.[307]
The working group óAK Vorratô, in collaboration with the Green Party, filed a constitutional challenge signed by 11,139 supporters on the 15th June 2012, which is currently being treated by the Constitutional Court.[308] Also the Freedom Party in Carinthia (FPK) filed a constitutional challenge against the Data retention directive on the 27th March 2012,[309] aiming for a similar result as in Germany, where the directive has been classified as non-constitutional-conform by the Court and thus suspended the implementation.

Results for Germany

The implementation of the EU data retention directive in Germany is based on the precondition that there is a national data retention directive, following from the EU initiative. Thus the development will be described as one line of progress here. All discussions about the EU data retention directive in Germany are proxy discussions, i.e. it is through the German data retention directive that the issue has become a public issue in the first place. Discussions on the EU directive are academic and surface almost exclusively when the preconditions of the German directive are addressed.
The law that implemented the EU directive on data retention has been approved by parliament on 9th November 2007. The protests began immediately and on different levels.
- *Civil society*: As early as 2006 citizens began to organise against the EU data retention directive. In Germany the *Arbeitskreis Vorratsdatenspeicherung (AK Vorrat)* was founded. It has since rallied against the directive and organised a set of very successful public protests, rallies and demonstrations. The biggest among them was in 2007 where 15,000 people walked the streets against the directive. In succeeding years further demonstrations followed. The motto under which they held their demonstrations and the discussion was Ăfreedom, not fearñ (*Freiheit statt Angst*). The initiative networked successfully and also filed a constitutional lawsuit in 2007. All in all 34,939 people signed the lawsuit - the biggest in Germany to date.
- Parliament / politics: The German directive was debated in parliament and support and opposition sometimes ran through a given party. Several members of the Bundestag filed separate constitutional lawsuits in addition to the *AK Vorrat*.
On 11th March 2008 the constitutional court limited the German directive in several ways. Revealing data was made more difficult for the criminal justice systems, including the need to produce a reasonable suspicion to a court and to demonstrate that such data is the only way of investigating the crime or suspect. In 2010 the *Verfassungsgericht* ruled the German directive, which was a direct implementation of the EU directive, as unconstitutional. The EU was of a different opinion and claimed that it was not in the courtsô power to decide upon the implementation in German law. A new German directive is now under construction and has yet to be produced and brought to parliament. In 2011 a new directive was presented but has not passed either house of parliament to date. The EU reprimanded Germany for not having implemented its directive in 2011. In 2012 the discussion has died down considerably. The *Deutsche Juristentag* now supports the implementation of the EU

[305] Der Standard 31st March 2012 Österreichweite Proteste gegen Vorratsdatenspeicherung http://derstandard.at/1333184930550/Farewell-Privacy-Oesterreichweite-Proteste-gegen-Vorratsdatenspeicherung 08.04.2013
[306] ORF 1st April 2012 Demo gegen Vorratsdatenspeicherung http://ooe.orf.at/news/stories/2527248/ 08.04.2013
[307] Futurezone 20.04.2011 Staat behandelt Bürger wie Terroristen http://futurezone.at/netzpolitik/2768-staat-behandelt-buerger-wie-terroristen.php 08.04.2013
[308] https://www.verfassungsklage.at/ 08.04.2013; Der Standard 15.06.2012 Scheibtruhenweise Klagen gegen die Vorratsdatenspeicherun http://derstandard.at/1339637967615/Scheibtruhenweise-Klagen-gegen-die-Vorratsdatenspeicherung 08.04.2013
[309] Kleine Zeitung 27th March 2012 FPK bringt Verfassungsklage ein http://www.kleinezeitung.at/allgemein/multimedia/2981497/verfassungsklage-fpoe-ueber-kaerntner-landesregierung.story 08.04.2013

directive and wants to have it approved as soon as possible. Some politicians want to even go further in the German directive and retain data in all cases, supporting a total surveillance of all communications just in case. Although the effectiveness of the directive and its measurements have yet to be proven, data retention is still seen as a key to crime prevention, crime fighting, especially terrorism, and finds large support among security oriented politicians and member of the security apparatus (police force and others).
The civil society protests are still on-going and have indeed made an impact to date. A final implementation has yet to be achieved and it seems safe to say that any attempt to do so will give rise to new protests and new lawsuits. The discussion of the directive was covered by all major media in Germany throughout. Although it was controversial, the media seemed to favour an oppositional point not supporting the directive, quoting arguments that were critical and went beyond the Ăcatch the terroristsñ lingo.

Results for Slovakia

There were no public protests and debates on the implementation of the directive. However, there was a considerable political and legal debate during the implementation of the directive in 2007 that was covered in the national media. Slovakia was one of the nine EU countries that did not ask to postpone the application of the 2006 directive. The directive was to be implemented through an amendment to the 2003 law on electronic communications with draft law, prepared by the Ministry of Transport, released in early 2007. During the consultation phase, where all relevant governmental ministries and agencies may propose their amendments and objections, the Interior Ministry, together with intelligence agencies, proposed several changes to the draft. In essence, they asked that police and intelligence agencies should have constant access to databases of telecommunication operators. The language of the proposal was very broad and suggested that the Interior Ministry asks for constant access to all data covered by the Article 5 of the directive. The critics, that included two smaller coalition parties, media, the Slovak DPA, but also mobile operators, pointed out to the fact that such general access is in direct opposition to the language of the directive suggesting that data are provided only "in specific cases". Also, especially national media pointed out the complicated history of information leaks in Slovakia and the role of intelligence agencies in these cases. As to "prove" the point, in May 2007, hundreds of protected phone numbers including phone numbers of the Interior Minister and around 700 phone numbers used by Slovak Information Service310 were listed in a free online phone book. The case was never successfully investigated. After several delays the Slovak government approved the amendment in August 2007, without including proposals by the Interior Ministry. The coalition parties agreed that they would return to dismissed proposals when preparing new legislation that was going to overhaul the country's intelligence agencies. The legislation has not been prepared to date (May, 2013). The amendment that implemented the 2006 EU Directive on Data Retention was finally approved by the Slovak parliament in December 2007. The media declared a "defeat for Big Brother" and pointed out that the parliament also changed a proposed period for data retention from two years to six months for Internet communication and to 12 months for other forms covered by directive.[311]

[310] The leak was covered in all national media, see TV Markiza, V internetovom telefónnom zozname sa objavili ļísla na viacerých ļlenov vlády a zamestnancov SIS, 21/05/2007
[311] See for example: Daily Hospodarske Noviny, "VeĎký brat musí priġmúriŠ jedno oko" (Big Brother Will Not See Everything), 14/12/2007, p. 5

9.1.2 Public debates on surveillance

Guiding question: Can you identify any other topics/events with a focus on surveillance surfacing in public debates?

Results for the UK

In the UK there have been a number of surveillance-themes that have stimulated public debate. Examples include: CCTV surveillance in public places and its use at major events such as demonstrations and crowd control at sporting events; the growing use of social media sites for unintended purposes - such as the monitoring of the social activities of employees by employers or potential employers; the growing use of social media to incite others to riot; the use of social media and CCTV to identify rioters;[312] the use of social media either openly or by ótrollsô to launch personal attacks on individuals; the growing acceptance of smart cards; the repeated attempts by the UK Government to use the Data Retention Directive Regulations as a means of requiring third party Communications Service Providers to collect and supply to the Government, various forms of communications data such as emails and mobile phone records (also colloquially referred to as the óSnooperôs Charterô).[313] However, in this section we concentrate on one ósurveillanceô topic that produced a good degree of public debates ï the unsuccessful attempt in the UK to introduce a national ID card scheme. The Identity Cards Act was passed by the Labour Government in 2006[314] and immediately opposition to the act questioned its purposes, the necessity for every citizen to obtain one and the cost of buying a card and indeed the cost of the entire scheme. The Labour Government insisted the Act would help to secure the UK against potential acts of terrorism.[315] The Government failed to win the public debate however,

People do not want the state keeping information on its citizens for some ill-defined and unproven benefit. Fewer than 15,000 people have bought an ID card since last November ï and around 3,000 of those were issued free to workers at Manchester and London City airports.[316]

In 2010 the then new Conservative/Liberal Democrat Coalition Government, as one of their first announcements, scrapped the legislation.

The government began the process of scrapping identity cards by introducing the Identity Documents Bill to Parliament on 26 May 2010. The bill made provision for the cancellation of the UK National Identity Card, the Identification Card for EEA nationals and the destruction of the National Identity Register. [317]

Paradoxically, however, the coalition Government announced details in October 2012, to introduce another form of a national identity scheme, where citizens could use their mobile phone or other forms of social media as a means of gaining access to publically available services,

óPeople wishing to apply for services ranging from tax credits to fishing licences and passports will be asked to choose from a list of familiar online log-ins, including those they already use on social media sites, banks, large retailers such as supermarkets, to prove their identity.ô[318]

---

[312] England riots: Police release first CCTV suspect images: BBC News, http://www.bbc.co.uk/news/uk-england-london-14462271, 9.8.11, Accessed: 14.3.13

[313] Snooper's charter rests on 'pretty heroic assumptions', MI5 boss told MPs: The Guardian online, 5.2.13: http://www.guardian.co.uk/law/2013/feb/05/snoopers-charter-pretty-heroic-assumptions?INTCMP=SRCH Accessed: 14.3.13

[314] The UK National Identity Cards Scheme: http://www.homeoffice.gov.uk/agencies-public-bodies/ips/about-us/suppliers/identity-cards/ Accessed: 14.3.13

[315] ID cards 'will not stop terrorism' The Guardian, 27.4.2004, http://www.guardian.co.uk/world/2004/apr/27/september11.usa Accessed: 14.3.13

[316] ID cards: gone for good. The Guardian, Damian Green, 9.6.10. http://www.guardian.co.uk/commentisfree/libertycentral/2010/jun/09/id-cards-damian-green Accessed: 14.3.13

[317] The UK National Identity Cards Scheme: http://www.homeoffice.gov.uk/agencies-public-bodies/ips/about-us/suppliers/identity-cards/ Accessed: 14.3.13

[318] National 'virtual ID card' scheme set for launch (Is there anything that could possibly go wrong? Ian Burrell, The Independent, 4.10.12

It remains to be seen whether or not these latest proposals will be accepted by the UK public, which is arguably becoming increasingly ósocialisedô in their apparent acceptance of the use of ósmartô cards in their business and social transactions.

Results for Italy

Beyond events focused on surveillance and/or resistance to specific surveillance practices, there are at least three topics that have emerged in public debates:

- the growth of surveillance cameras (from the late 1990s until today),
- Telecom Italia wiretapping scandal (2006),

and, more recently,

- financial surveillance (2012).

Of the three above-mentioned topics, only for the first is it possible to identify relevant active NGOs, as described in section 4.5. Additionally, as far as surveillance cameras are concerned, the Italian DPA was the only relevant public stakeholder which, in a decade, issued a Decalogue and two provisions on video surveillance that helped, at least, to shed light on the growing number of cameras. In all cases, public involvement and reactions from NGOs were almost non-existent.

Despite the ñsilentò growth of surveillance cameras in Italy[319], the early growth of legal regulation of CCTV suggests that this was an issue of concern for the DPA and for the general public alike. Moreover, as described in section number 4.1, the use of surveillance cameras at specific locations, such as schools, fostered both public debate and reactions from the DPA.

At the end of the 90s, a new approach to urban security fostered an increasing demand from the citizens to live in safer cities. While local governments and mayors gained power over policing, surveillance technologies, in particular CCTV, seemed to offer relatively rapid answers to new vulnerabilities such as migration flows. Moreover, the politics of fear towards the ñotherò was fuelled by movements, like the political party Northern League, who often called urban security into question and asked for ñhard measuresò to deal with security-related problems.

In the late 90s and in the first decade of the new millennium, the approach to video surveillance was twofold: if, on the one hand, the DPA shed light on the right to the privacy of the citizens and pointed out potential social implications of this tool and the need for a less technologically driven approach to security, on the other, the new ñsecurity narrativeò increasingly revolved around the right to live in safer cities. CCTV, thus, became a political argument used in electoral campaigns: security and video surveillance were often depicted as two sides of the same coin. The argument was framed in terms of a trade-off between surveillance and privacy and the topic of security and surveillance colonised the political debate until the elections in 2008[320].

The terrorist attacks in the USA and in Europe paved the way for security regimes, which relied more on the promises of visual technologies than on data pertaining to their effectiveness. The public debate, though, was characterized by a top-down approach: while, as mentioned, the President of the DPA raised concerns about the increasing number of cameras in Italian cities as early as 2000, politicians used the argument of video surveillance in order to show that they were trying to deal with security-related problems through the installation of more cameras. Therefore, the mainstream media touched upon this issue from perspectives that did not focus on perceptions of security and/or insecurity of the lay citizens but rather on what had or had not to be done to solve security problems[321].

In 2008 a short documentary on the relationship between video surveillance and the urban milieu

---

http://www.independent.co.uk/news/uk/politics/national-virtual-id-card-scheme-set-for-launch-is-there-anything-that-could-possibly-go-wrong-8196543.html: Accessed: 14.3.13

[319] Fonio, Chiara, ñThe Silent Growth of Video Surveillance in Italyò, *Information Polity*, Vol. 16, Number 4/2011, pp. 379-388.

[320] http://www.lastampa.it/2013/02/22/italia/politica/la-sicurezza-sparisce-dalle-elezioni-ma-la-criminalita-e-in-aumento-I5I5jRDM4oowPDtKoNSHON/pagina.html, 22 February. 2013

[321] For instance: http://www.firenzepost.it/2013/02/20/piu-telecamere-per-la-sicurezza-a-firenze/

entitled ñ*Occhi su Roma*ò (Eyes on Rome) was released but it did not help to fuel the debate on the social costs of surveillance cameras despite the critical approach of the director.
When the economic crisis hit the country, social economic insecurity became the main ñhot topicò and it is still a crucial and unavoidable issue that minimizes the visibility of any other topics. Additionally, the public debate on, for instance, the installation of new surveillance cameras within specific urban contexts, seems to be more local than national as recently demonstrated by a massive surveillance-camera project called ñsafe cityò. At the beginning of March 2013, the city council of Catanzaro (Calabria) announced that around 900 military Israeli surveillance cameras bought from Bunker Sec will be installed across the city[322]. This massive surveillance project has not emerged in mainstream media yet, despite privacy concerns raised by associations and citizens.
However, before the economic crisis, surveillance and privacy issues did become a hot topic when the Telecom wiretapping scandal was exposed in 2006 during the investigations on the Abu Omar extraordinary rendition case[323]. The scandal entailed a massive illegal wiretapping and surveillance of telephone networks carried out by Telecom Italia over at least 10 years (mid 90s-mid 2000s). It is often referred to as the SISMI (Military Intelligence and Security Service) -Telecom scandal as the ñsurveillance programò was run by Marco Mancini, a high-ranking officer of the SISMI, arrested for the involvement in the kidnapping of Abu Omar, Giuliano Tavaroli, chief of security of Telecom Italia and Emanuele Cipriani, a private detective.
More than 5,000 people were spied upon and thousands of dossiers documented that, while the target of surveillance was enormous, the aims were not always clear-cut. Dossiers on major Italian figures (e.g. politicians, managers, former ministers) could have been used to blackmail them and were collected through Cipriani, ñone of the most significant providers of outside services to the Security Functionò of Telecom Italia[324]. The complex and multi-layered patchwork that emerged from the spying scandal received a significant amount of national and international media coverage. The case drew the attention of the most important Italian newspapers, such as *Corriere della Sera* and *La Repubblica* which were also targets of surveillance. In particular, the computers of two reporters of *La Repubblica*, who had broken the so-called Yellowcake (Niger uranium) forgery story and the involvement of the SISMI in it, were hacked by the Tiger Team, namely a team of informatics and computer experts based at Telecom Italia.
The ñspy storyò, thus, involved a wide range of surveillance technologies as well as the involvement of many people, institutions and private companies which played their role in collecting data and assembling illegal dossiers on prominent Italian figures. As pointed out by the EDRI (European Digital Rights Institute) ñthe telecom wiretapping scandal has shown that private companies and reporters in connection with SISMI were able to access information regarding Italian citizens, using the system in place for legal wiretappingò.[325] Since 2005, in fact, the company has changed its structure and improved judicial authoritiesô services, in particular, mandatory services for judicial authorities. However, at some point legal tapping and illegal tapping activities seemed to blur. Moreover, journalists from the weekly *L'Espresso* proved that a surveillance system called Radar was used by Telecom to spy on mobile phones without leaving any traces[326]. The Italian DPA also started an investigation into Telecom.
Nevertheless, despite the media coverage, the wiretapping scandal did not lead to any direct involvement of lay citizens in public events against, for instance, illegal surveillance. This is perhaps

[322] http://www.corrieredellacalabria.it/stories/politica/13159_gli_occhi_israeliani_su_catanzaro/. 16 March 2013.
[323] The Milan imam Abu Omar was an Egyptian with a refugee status in Italy who was illegally arrested by CIA agents, transferred to Egypt where he was interrogated and tortured for more than one year (Mazza, Caterina, The Abu Omar Case and Extraordinary Renditionò , *Central European Journal of International and Security Studies*, Volume 6, Issue 2, pp. 134-159.
[324] http://www.sec.gov/Archives/edgar/data/948642/000094864207000006/t6k070222n01.htm
[325] http://www.edri.org/edrigram/number4.15/italy
[326] http://www.adnkronos.com/Archivio/AdnAgenzia/2006/06/15/Economia/Telecomunicazioni/TELECOM-LESPRESSO-RADAR-ERA-NOME-BANCA-DATI-PARALLELA-UTENTI-TIM_102449.php

due to the fact that the Telecom Italia scandal drew a picture, which emphasized that surveillance was carried out to spy on politicians, magistrates, journalists or well-known soccer players. The everyday lives of ordinary people were not the primary target of wiretapping.

More recently, another surveillance-related topic has been covered by national media and has raised privacy concerns. In an effort to combat tax evasion, a tax compliance policy called ñredditometroò, or income measure, was renewed in 2010 and the range of expenditure items examined significantly expanded in 2013. This measure aims to evaluate the consistency of the expenses of individuals to their income by examining expenditures in more than 100 categories, from food to leisure pursuits. Italian authorities, as reported also by the BBC, have been accused of ñrestoring police state-style tacticsò[327] as families spending patterns are scrutinised in order to find incongruities, namely if the tax payersô spending appears to be more than 20 percent greater than the income declared.

The well-known Italian columnist Piero Ostellino wrote, in an article published in *Corriere della Sera*, that the introduction of this tax compliance policy has restored a surveillance police state similar to the 20th century totalitarian regimes[328]. Privacy concerns were raised along with concerns related to the main logic behind this system, that is that if incongruities are found, taxpayers are guilty until proven otherwise. This is called ñdouble-contradictoryò for the alleged evaders: ñthe taxpayer put under observation will be entitled to give clarifications on any allegations made against him. If his explanations are not sufficient, he will then be called to discuss the survey resultsò. [329]

Additionally, uncertainties pertaining to the implementation arose in a trial in Naples in February 2013 when a taxpayer demanded an ordinary judge be prevented, in absence of an intervention by the tax police, from checking and analysing the expenses since ñotherwise the tax agency would become aware of all aspects of his/her daily life, thus hurting not only the right to privacy but also to individual freedomò[330]. According to the taxpayer, the rights to privacy and to individual freedom were at stake and the judge, on the basis of an interpretation of the Constitution, ordered the agency not to gather information pertaining to the application of the income meter.

As argued by The Economist, the redditometro can be described as big government who meets big data[331] as it involves large databases and data matching through ñhuge computing powerò. In particular through a software called ñSerpicoò or ñfiscal big brotherò used by the Italian Revenue Agency which analyses and matches 24,200 pieces of data per second directly from banks, insurances companies archives, etc. through 2000 servers[332]. Therefore, the legal principle of bank secrecy has faded away in the name of fighting tax evasion. Although this is perhaps the surveillance measure within the national context, which is more controversial from a privacy standpoint, it seems that there is a lack of transparent public debate on fiscal surveillance.

Results for Austria

Besides the data retention directive in the recent past a group of activists providing citizens with fake loyalty cards for one of Austriaôs biggest supermarket chains captured the attention of mainstream media. The website http://nocard.info hosted a platform in early 2014 generating loyalty cards *for costumers who were upset about the tracking capacities of loyalty cards*[333], argued one of the anonymous hosts of norcard.info in a recent interview. Through Twitter and intensive media coverage in some of Austriaôs most popular newspapers nocard.info became a popular service in early 2014 and

[327] http://www.bbc.co.uk/news/business-21064030
[328] http://www.corriere.it/editoriali/13_gennaio_06/Il-redditometro-del-dottor-stranamore_13f05832-57ea-11e2-9a31-1eca72c52858.shtml. 6 January 2013
[329] http://www.thisisitaly-panorama.com/top-stories/redditometro-and-redditest-new-weapons-to-fight-tax-evasion-in-italy/. 23 November 2012
[330] http://www.ilsole24ore.com/art/english-version/2013-02-23/sterile-substitute-role-judges-043950.shtml?uuid=AbojoSXH. 23 February 2013.
[331] http://www.economist.com/blogs/schumpeter/2013/01/tax-evasion-italy . 8 January 2013
[332] www.inps.it/portale/image.aspx?iIDRassegna=4373
[333] http://futurezone.at/digital-life/nocard-kundenkarten-haben-sicherheitsproblem/47.137.900 20 January 2014

the loyalty cards were debated on a different level in the general public. In summer 2014 the platform was not available any more after the supermarket chain announced intentions to sue the anonymous operators of the platform because of attempted fraud. The impact of nocard.info can be described as fairly high as it was the first time since the introduction of loyalty cards in Austria that awareness for potential security risks and the infringement of private data was raised amongst the general public.

Results for Germany

In Germany, a big issue is and has always been the *surveillance of workplaces* respectively workers. In 2008, discount supermarket chain ñLidlò has been accused of spying extensively on their employees: ñWho went to toilet at what time? Which employees may have a relationship with each other? Who did they talk to on the phone during a break? About what?ò (Spiegel, 26.3.2008).

Besides this, surveillance is a recurring topic after some specific types of crime have been reported:

- *Child abuse*: There are on-going debates about how to surveil convicted or potential suspects of child abuse. In 2007 there were, though only little, thoughts about having an online mapping system, where the residency of persons who had been under suspicion could be tracked, corresponding to similar websites that existed in the US at that time. Politicians are engaged in these debates every time another crime is committed. The last incidence fuelled the debate about electronic tags.[334]

- *Brutal violence on the streets/terroristic attacks*: After each occurrence of brutal violence in public places[335], increased monitoring via CCTV is demanded by politicians. The day after the Boston bombing, current home secretary Friedrich was quoted as follows: ñWhat happened in Boston shows again how important it is to have surveillance of public places, in order to solve crimes of the most violent types. This is why we are cooperating with railway companies to have more CCTV at stations.ñ (Spiegel, 20.4.2013)

CCTV in general has only recently become a bigger topic in political debates as well as in the media (see Q7). Between January and April 2013 there were 43 enquiries concerning CCTV in all kinds of political institutions, more than in other years during the same period. The enquiry concerning the situation in Bavaria for example showed a massive increase of CCTV cameras in operation. Since 2008, the number of video cameras went up from 12.000 to about 17.000 in 2012. Politicians from the green party stated in this respect, that ñproportionality is all goneò in this field (SZ, 27.2.2013).

Results for Slovakia

The topics connected to "new" surveillance surface only sporadically and are not usually followed for longer period of time by public and the media. One bigger case worth mentioning that was followed by the national media for a few weeks involved the national census in 2011, organized by the Statistical Office of the Slovak Republic.[336] A few days before census forms were distributed, a "blogger and security expert" (in his own words) pointed out to a potential misuse of census data because their anonymity was compromised by a unique numerical code used on every census form[337]. The blogger involved a national TV channel and filed an official complaint against the Statistical Office with the Slovak DPA. The DPA released a press statement a couple days later (only a few days before the official start of the census), in which it asked the Statistical Office to fully "inform the residents of Slovakia that the data collected for the 2011 census is not anonymous and to cancel residents' obligation to place the numerical code on their respective census form." The

[334] http://www.tagblatt.de/Home/nachrichten/ueberregional/blick-in-die-welt_artikel,-Prozess-gegen-Sexualstraftaeter-loest-Debatte-um-Ueberwachung-aus-_arid,199827.html

[335] See the paradigmatic case of Dominik Brunner (2009): http://spon.de/verVn, two cases in Berlin (2011): http://spon.de/veOPo and (2013): http://www.focus.de/politik/deutschland/nach-toedlicher-alexanderplatz-attacke-innenminister-will-mehr-videoueberwachung-in-deutschen-staedten_aid_843028.html

[336] Slovak Spectator, 30/05/2011, Anonymity of census data questioned.

[337] Original blog post that started controversy, https://www.iseco.sk/scitanie-2011/, In Slovak

Statistical Office responded with its own statement, calling the DPA's release "manipulative" and accused the DPA of endangering the results of the census. After the intervention of the Prime Minister I. Radicova, the DPA softened its stance and later cancelled it after formal review by the Attorney General's Office. The controversy influenced returns of the census forms, especially in Bratislava, in which almost 20% of residents did not return their forms.[338]

9.1.3 Stakeholders active in the public debates on surveillance and democracy

Guiding question: Identify relevant stakeholders (individuals, CSOs NGOs etc.) involved in this debate.

Results for the UK

In the UK the two highest profile stakeholders highlighting surveillance issues, human rights and civil liberties are probably *Statewatch* and *Liberty*. Both of these organizations appear regularly in the UK media.

Statewatch

Statewatch is a voluntary group made up of lawyers, academics, journalists, researchers and activists. The groupôs interests relate to the state, justice and home affairs, civil liberties, accountability and openness. One of their main modes of communication is their website, where they host investigative papers and articles. Members of the group also publish in national newspapers and make occasional television appearances. The groupôs flagship publication is the óStatewatch Bulletinô. The bulletin is published quarterly. The Statewatch website also has a database of ómore than 25,000 articles, references and documentsô referring to issue of state and civil liberties. [339]

Liberty

Liberty is an organization concerned with civil and human rights and freedoms in the UK. Liberty has more of a judicial background than Statewatch and the majority of its ópublic facingô staff have experience or training in Law. The organizationôs purpose is to ensure the protection of basic rights and freedoms in the UK óthrough the courts, in Parliament and in the wider communityô. Highest profile of the Liberty staff is Director Shami Chakrabarti; she frequently appears in the UK media and is vocal and outspoken on issues relating to UK civil rights. Probably best known for her opposition to the Iraq War, she also champions infringements on human rights being affected by a host of new Governmental initiatives, for example, the Communications Bill.

Privacy International (PI) is a non-profit company that promotes and preserves the right to privacy across the world. PI based in London has organised campaigns and initiatives in numerous countries. PIôs work includes the monitoring of how surveillance technologies are being employed by the state, for instance one recent focus has been "IMSI catchers" masts that look and act as standard mobile phone masts, but house malware ï a software that can allows its operator to control a target's computer, while remaining undetected.[340]

Big Brother Watch (BBW) illuminates policies, which may threaten privacy, freedoms and civil liberties ï with an emphasis on questioning the motives and creation of a ósurveillance stateô. Central to their concerns is óexposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal

[338] For more on influence see, SME, http://www.sme.sk/tema/scitanie-obyvatelov-2011/, In Slovak
[339] See, http://www.statewatch.org/
[340] See, https://www.privacyinternational.org

informationô. BBW campaigns to promote an increased awareness of the rights to personal data and for a greater public awareness of the implications and uses of personal data. The group is relatively unusual in that is has a distinctively central right political agenda ï most NGOs of this nature in the UK are central-left. [341]

Open Rights Group (ORG) interests lie with issues of freedom of expression, privacy and consumer rights online. They state of their aims, ôWe campaign to change public policy whenever your rights are threatened, by talking to policy-makers, informing the public through the media, and mobilizing our supportersô. ORG is non-profit organization based in London and was founded in 2005 by digital activists. The NGO is voluntary staffed by campaigners and interns.[342]

Links with other civil society actors

It is difficult to establish if there are links to civil society actors and if there are established links between the NGOs. Presumably membership of organizations is not exclusive and there are many who have membership of a number of NGOs. However, what we would surmise is that there is a degree of competition between the NGOs as most are registered charities and reliant on their own subscriptions and donations. While most of the NGOs do on occasion link-up (for example, in opposition to the Iraq War) for the most part they tend to stick to their specialisms or area of interest. NGOs are vying for funding from the same pools of money ï i.e. funding bodies, wealthy benefactors or donations. They do, however, have external links with for instance their or other international or regional branches, or on occasion links to International organisations with common interests.

Results for Italy

The Telecom wiretapping scandal and financial surveillance caught public attention but did not fuel critical reactions as such. However, in the first decade after the year 2000, it became apparent that the growth of video surveillance in Italian cities was of particular interest to left-wing social movements, which tried to raise awareness on video surveillance through resistance. Despite their critical approach, the general level of awareness remained limited and fragmented. However, it seems worth looking at two active social movements.

Inventati/Autistici[343], for instance, is a ñcollectiveò ï as they defined themselves ï started in 2001 that has been dealing with surveillance, technology and the right to privacy. One of their aims is to raise awareness on these issues and they did engage with video surveillance through a document on CCTV (ñVideosorveglianzaò) released in the early 2000s[344]. Data on surveillance cameras drew from ñspialaspiaò (spythespy) and Tactical Media Crew[345] both active in the late 90s and at the beginning of the 2000s. In particular the website ñspialaspiaò was the first public attempt to map video surveillance in Italian cities. The above-mentioned document focuses on four main themes: a) video surveillance as ñbig brotherò, b) news on CCTV in Italy, c) resistance to CCTV, in particular how to disable or destroy the cameras and d) how to map video surveillance. There are no descriptions of actions and/or events against surveillance cameras, but the idea of resistance against the electronic eyes through a detailed documentation of the location of CCTV has been carried on by other social actors. For instance, the project Anopticon[346] has been, and is still, very active in mapping surveillance cameras in Venice. Moreover, a mobile app (Anopticon Mobile) for smartphones can be downloaded from the website. This app enables mapping of public surveillance cameras on Google maps and citizens have used this tool to map CCTV in many Italian cities.

Currently, the Anopticon project is the most active within the national context. However, more than

[341] See, http://www.bigbrotherwatch.org.uk
[342] See, http://www.openrightsgroup.org
[343] www.inventati.org
[344] http://www.inventati.org/reginazabo/videosorveglianza.pdf
[345] www.tacticalmediacrew.org
[346] www.tramaci.org

being involved in ñeventsò, the main aim of Anopticon is raising awareness through either the mapping of all public surveillance cameras within urban contexts or through publishing relevant documents on surveillance on the website. Therefor, this specific stakeholder was not involved in events against surveillance but the project initiator took part in public debates focused on video surveillance such as e-privacy[347] and freedom not fear[348]. Nevertheless, these events had a limited impact and media coverage was almost non-existent. For instance, in the last winter edition of freedom not fear held in Venice and focused against CCTV, very few people showed up and the event did not make national media.

Another stakeholder who is involved in the surveillance debate, but only partly concerned with the above mentioned topics, is Anonymous Italy[349]. Like all Anonymous groups, the Italian group is also active against, *inter alia*, state surveillance and the massive use of surveillance technologies. In 2012, a campaign named #AntisecITA[350] started. At the core of the so-called ñoperation policeò lies the exposure of files held by law enforcement that deal with the wiretapping of activists, undercover activities and surveillance technologies. Anonymous retrieved 1.35 Gigabyte, 3,500 files, from the Italian State Police, among which there are also files about the Telecom Italia wiretapping[351]. This event or operation against the police and the use of surveillance technologies to monitor activists made national media but, once again, did not fuel public debates by lay citizens on the use on surveillance

Results for Austria

In Austria you wonôt find well-established organisations as Statewatch or Liberty like in the UK but there are a number or similar (smaller) groups active in the public debate on privacy, data protection and fundamental rights with regards to the use of the Internet. All of them are in general concentrating their efforts on certain aspects of data protection and privacy protection (e.g. on data retention).

AKVorrat (www.akvorrat.at)

Was the most prominent actor in the public debate on privacy and fundamental human rights during the time that the data retention directive was actively used by Austriaôs Law Enforcement Agencies. AKVorrat, a group of IT specialists and lawyers, filled several complaints to the higher court of justice against the data retention directive. Especially during 2012 AKVorrat was establishing itself as a citizens movement actively campaigning against the data retention directive. Since the Federal Constitutional Court suspended the directive in June 2014 it has become quieter again around the AKVorrat citizens movement.

Netzfreiheit (www.netzfreiheit.org)

The Article 5 (2) (b) Directive 2001/29/EC on the enforcement of intellectual property rights is at the moment (Summer 2014) highly debated in Austria. A group of Internet activists founded the platform www.netzfreiheit.org (net freedom) to campaign for a free and open Internet. The group filled several complaints against the Austrian Ministry of Justice and is prominently featured in the network policy columns of Austriaôs high quality newspapers.

Europe vs. Facebook (www.europe-v-facebook.org)

The right to data protection is conceived as a fundamental right in the European Union. The platform www.europe-v-facebook.org is hosted by the Austrian Student Max Schrems who ï through its activities (filling 22 complaints against Facebook in Ireland) ï became an ñ*Internet celebrity in Austria*ò. The group is frequently featured on the public youth radio station (www.fm4.at) promoting

[347] http://e-privacy.winstonsmith.org
[348] http://www.freedomnotfear.org
[349] http://anon-news.blogspot.it
[350] http://operation-police.blogspot.it
[351] http://www.par-anoia.net/releases2012.html#poliziadistato

their ideas and trying to raise awareness amongst the younger generation to be careful with what kind of information they share on social media platforms.

Results for Germany

Workplace surveillance is a topic only really taken up by the German labour union ï no other institutional or individual actors represent citizensô interests with much legitimacy and power.

Child abuse: German Ministery of Family Affairs promoted the idea of closing certain websites for German visitors (ñZugangserschwerungsgesetzò, 2009), which created massive protest from sides of the Internet community. ñThe 13 Lies of Zensursulaò[352] were criticised harshly, and lots of protest was organised, e.g. a demonstration, which attracted ten thousand people in Berlin (September 2009). The ñZensursulaò-Case created huge and sustained awareness about Internet restrictions. In 2012 the big demonstrations against ACTA built up on the already existing knowledge. Those were supported by the Pirate Party as well as lots of different (I)NGOs like Avaaz.org, Anonymous, ñStopActaò as well as parts of the AK Vorratsdatenspeicherung. CCTV Camera Surveillance is not so much an event-based phenomenon, but more a long term-development as described above. Therefore organizing single protest waves very much depends on finding concrete changes of practice in the area of CCTV, to launch protests. This has been the case with the European Union INDECT-Project that examines the possibilities of connecting data from different sources to then control and pilot mobile cameras. The first demonstrations against INDECT were organized by Anonymous and FoedBUD, together with the Pirate Party in 25 cities across the country.[353] These however did not attract as many citizens as did the ACTA case, the last demonstration in Munich e.g. in March 2013 only attracted about 25 persons.

Results for Slovakia

The only "visible"[354] NGO that deals with data protection, privacy and surveillance is EISI, (European Information Society Institute, http://eisionline.org/. The NGO focuses mostly on the overlap of technology, law & information society that includes Internet law and Intellectual Property Law. It was EISI that prepared a draft of a constitutional complaint against data retention that was adopted by a group of Slovak MPs.

Governmental

- The DPA ("Urad na ochranu osobných údajov), http://www.dataprotection.gov.sk
- Intelligence agencies: Slovak Information Service, ("Slovenska Informacna Sluzba"), http://www.sis.gov.sk; Military Intelligence, ("Vojenske spravodajstvo")
- The Ministry of Transport, Construction and Regional Development of the Slovak Republic, ("Ministerstvo dopravy, vystavby a regionalneho rozvoja"), http://www.telecom.gov.sk/index/index.php?lang=en
- Attorney General Office, "Generálna Prokuratúra SR",

Business

- Mobile operators: Orange Slovakia, http://orange.sk; Telekom, http://www.telekom.sk; 02 Slovakia, http://www.o2.sk
- Cable Internet: UPC Slovakia, http://www.upc.sk

NGOs

- Aliancia Fair-Play, http://www.fair-play.sk
- Transparency International Slovakia, http://www.transparency.sk
- European Information Society Institute, EISI, http://eisionline.org

[352] https://netzpolitik.org/2009/die-dreizehn-luegen-der-zensursula/

[353] The full lost of registered demonstration can be found here: http://www.stopp-indect.info/index.php/de/opindect

[354] However, EISI is widely known and it was featured in only few stories. Based on their website, it is also a very small NGO, composed only of two lawyers and one IT expert.

9.1.4 Role of the police in the national debate on surveillance

Guiding question: What is the role of the police in the field of surveillance and crime fight? Do police authorities develop awareness for the problematic of surveillance?

Results for the UK

In the UK, there are 3 main territorial Police forces covering England, Wales, Scotland and Northern Ireland. Additionally, there are specialist forces covering transport, civil nuclear sites, Ministry of Defence sites, some ports, parks, airports, and various localised branches with responsibility for tunnels, cathedrals and markets. The UK territorial Police, much like all police forces, rely on surveillance technologies and practices in combatting crime. Other surveillance ôactorsô also participate in policing, from locally based neighbourhood watch volunteers, to Community Planning partnerships, to the Crown Prosecution Service (England and Wales), to the Home Office and to ôspecialô constables.[355] Nevertheless, we want to turn to CCTV in giving an understanding of surveillance and the interrelationships between the police, actors and technologies in the UK.

CCTV, the Police and Criminal Investigations

Since the early 1990s, when CCTV first started to be rolled-out across town and city centres[356], it has become an increasingly important part of the UK Police ôtoolkitô. Within criminal investigations CCTV has achieved early ôguiltyô pleas and has reduced time spent in court and preparing for court by the Police and the criminal justice officials.[357] The importance of CCTV is stated in the standard ôPolice Reportô issued by The Crown Prosecution Service (England and Wales), when officers interview suspects, they should note not just the availability of CCTV evidence, but the defendantôs ôresponse/reactionô to it.[358]

CCTV and the Influence of Other Actors

It is also worthwhile noting the historical role which central government in the UK has played in the advancement of public space CCTV systems, and the importance of how its legacy influences the operational role which the Police play today in its use. From the early 1990ôs onwards, successive central governments have invested heavily in the infrastructure of new CCTV systems, thus allowing them to have a major say in how local authorities would operate and deliver these new systems[359]. It became politically expedient to publically support CCTV and for politicians to be seen to be ôtough on crimeô[360] with central government influencing operational guidance on the use of CCTV systems and establishing their role as the leading player in the creation of policy networks, thus influencing the role which the Police could play.[361] In Scotland, for example, the Police are not in direct control of the vast majority of local authority controlled systems. The future of CCTV in Scotland concern the age of the systems, and the lack of available funds to replace these systems, coupled with a drive from the Scottish Government to have standardisation of systems across the country to allow the sharing of

[355] Special constables are trained volunteers who work with and support their local police. They wear the same uniform as the police but have lesser powers that Police Officers (they cannot arrest for instance) and are usually deployed to deal with minor incidences and to patrol streets.

[356] Webster, William, ñCCTV Policy in the UK: Reconsidering the Evidence Base, *Surveillance & Society*, Vol. 6, No 1(2009) pp. 10-22, http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3400/3363

[357] Levesley, T., A. Martin, and G. Britain. *Police Attitudes to and Use of CCTV*, Home Office, 2005.

[358] http://www.cps.gov.uk/search.asp?mode=allwords&search=cctv&submit.x=0&submit.y=0 Accessed: 11.3.13

[359] Webster, William, ñCCTV Policy in the UK: Reconsidering the Evidence Baseò *Surveillance & Society*, Vol. 6, No 1(2009).

[360] Fussey, P., "New Labour and New Surveillance: Theoretical and Political Ramifications of CCTV Implementation in the UK", *Surveillance and Society* 2, no. 2/3, 2004:pp. 251-269.
Norris, C., and G. Armstrong. *The Maximum Surveillance Society: The Rise of CCTV*, Berg Publishers, Oxford, 1999.

[361] Webster, William, ñThe Diffusion, Regulation and Governance of Closed-Circuit Television in the UKò, *Surveillance & Society*, Vol.2 (2/3) 2002. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3376/3339

information, ó*to allow the police service and other partners to respond on a strategic level to major emergencies and the threat of terrorism*ô[362]

The Police and Surveillance at the Local Level

The Association of Chief Police Officers in Scotland, produced a Public Reassurance Strategy (2007) which recognises the value of,

ó*effective partnerships between the police, voluntary and community groups are a vital element in achieving meaningful improvements in the quality of life within communities. Organisations such as Neighbourhood Watch, which operates at national, regional and local levels, can provide a positive influence in creating safer communities.*[363]

The Public Reassurance Strategy also provides the chance for members of communities to volunteer for roles such as membership of the Key Individual Network,

By nature of their occupation or role within the community, some people are more sensitised to their environment and are more likely to notice changes in their neighbourhood. Examples of such people would be school janitors, shopkeepers and retired people. By regularly monitoring their views, the impact of police and partner interventions can accurately be assessed.[364]

Clearly, the Police have invested time and resources in promoting and developing ósoftô surveillance networks at the local level, through a variety of different types of contacts, which include: community wardens, neighbourhood watch volunteers, the Key Individual Network and through close links with the widely publicised and successful Crimestoppers service[365] which is a UK-wide charitable organisation providing a confidential and anonymous telephone service for people to report information about crime.

Results for Italy

In Italy there are various police forces each having both a specific status and structure. The most prominent forces are the State or National Police, which reports to the Ministry of the Interior, and the *Carabinieri* which reports to the Ministry of Defence and has a military structure. Moreover, there are other forces that deal with specific areas, such as the Financial Police, the Post and Telecommunication Police, the Border Police, Anti-Terrorism Police, Local and Mobile police units etc.

Their role in the field of surveillance and crime fighting is crucial but the extent to which they use surveillance technologies obviously depends on the area of concern. Put simply, they use surveillance according to the aims of the specific police force. For instance, public video surveillance to prevent and deter crime within urban contexts is used by both the State and Local Police but it is also used by the *Carabinieri*, Mobile units and the Anti-Terrorism Police, while Internet surveillance is mainly ï but not solely ï carried out by the Post and Telecommunication police in order to fight, *inter alia*, child trafficking and child abuse. Furthermore, the role of law enforcement agencies varies either at a local or a regional basis thanks to the so-called ñlocal security agreementsò (ñpatti per la sicurezzaò), namely agreements between the State and local authorities to deal with crime[366].

Pertaining to the debate on surveillance, there are at least two aspects that can shed light on the role of the police in the national debate: a) public events and b) communication with the public through their websites. As far as public events are concerned, law enforcement agencies do not seem to hold, for

[362] Justice Analytical Services: Strategic Report on Improving the Efficiency and Effectiveness of Public-Space CCTV in Scotland. 2009

[363] ACPOS, Public Reassurance Strategy, 2007, http://www.actiononviolence.co.uk/content/acpos-public-reassurance-strategy-2007. Page 6

[364] ACPOS, Public Reassurance Strategy, 2007, http://www.actiononviolence.co.uk/content/acpos-public-reassurance-strategy-2007. Page 6

[365] CRIMESTOPPERS: http://www.crimestoppers-uk.org/ Accessed 13.3.13

[366] The Constitutional Law no. 3 dated 18 October 2001 fully recognises self-government to local authorities.

instance, community meetings in order to explain how specific surveillance tools like surveillance cameras are used to enhance public safety before the system is operational. In other words, they do not promote ñsurveillance awareness debatesò but rather the use of surveillance tools by police forces is not problematized and, more often than not, the efficacy of these tools is not even questioned. Generally, it is taken for granted that law enforcement agencies use surveillance for security reasons, thus other issues, like the progressive erosion of privacy, are not considered as crucial as the right to live in a safe place. There might be exceptions (i.e. community policing that organizes local events in order to promote neighbourhood watch and/or meet citizens to listen to their concerns and explain the role of surveillance technologies) but the overall approach is top-down. Moreover, if there are events focused on surveillance tools, they are not for the ñlay citizenò as such, but rather for scholars and stakeholders active in the field of security[367].
Consequently, the communication with the public through their websites focuses more on surveillance tools in order to promote specific activities rather than trying to engage citizens in informed debates. For instance, on the National Police website[368] there are references to intelligence, surveillance-related activities and law enforcement databases but the emphasis is mainly on the important role of these tools to enhance security. As far as public events are concerned, references are to events where the activities of various police forces are promoted

Results for Austria

CCTV is generally speaking often introduced as a reaction to increased crime rates in a certain area of a city. In Austria the role of the police with regards to the use of CCTV in public spaces can be described as rather restrained. In 2014 there are 18 places all over Austria (approx. 8 Mio inhabitants) that are put under CCTV operated by the police. All of them are considered as hotspots for crime and are located in city centres all across Austria. These numbers are quite moderate in comparison to the development in other European countries in the past 20 years but it is unclear how many CCTV cameras are operating in Austria. The *AKvorrat* (see 10.1.3) an activits group similar to *Statewatch* in the UK assumes that an estimated number of 100,000 CCTV cameras are operating in Austria without being registered at the national data protection authority.

Results for Germany

The role of the police in the field of surveillance is most interesting when concerning their role in the national debate. And when asking about the awareness for the problems of surveillance, it becomes clear that the police has an ambivalent role, which shall be addressed here.

In general one can say that the police is eager to participate in new technological developments, which help them to do their work better. It is no surprise that the police and their lobbying agents were and are in favour of data retention to fight crime and terror; they are in general supportive of CCTV as they argue that it is a valuable means of crime prevention and helps them to convict suspects and eventually solve crimes. Debates around CCTV, data retention as well as the so-called *Online-Durchsuchung* (online search of suspected computers by way of a spying software) show their involvement and role quite clearly. The police are in almost all cases in favour of measures and adjunct technologies, if they see that it may support their work or fits in their lines of argumentation to fight crime. Police authorities develop awareness in regards to surveillance when it comes to so-called cybercrime within their crime prevention schemes that they offer to citizens and the wider public (cf. http://www.polizei-beratung.de/). Among the themes that they address are ***ñ****Danger on the Internet****ñ*** with subthemes such as phishing, viruses, trojan horse software, cybermobbing etc. One could argue this is where the police develops an awareness of surveillance and actually actively promotes

[367] For instance: http://italy.iir.es/Images/P5336_DEM.pdf
[368] www.poliziadistato.it

countermeasures in the context of crime prevention. On the other hand, on issues such as burglary, the police actively promote security measures that also involve surveillance technologies, such as video surveillance around the house. In the case of online issues, the police recently have sought after ways of using the social web for their fight in crimes. The surveillance of Facebook, and other social media to investigate and fight crime has become a new way as various official documents from local and federal parliaments in Germany show.

Results for Slovakia

Slovakian Police authorities are not very much involved in the *national surveillance debate*. For example the media debate surrounding use of CCTV in public in Slovakia is limited exclusively to their security and crime prevention role, without ever mentioning their effectiveness and privacy issues. Also, public CCTVôs are owned and operated by local police departments that are responsible to city/village councils and are not part of national police force.

9.2 ANNEX II ï INTERVIEW DATA

9.2.1 Interview guideline: questions

Reinhard Kreissl, Alexander Neumann

Initial Questions

The Initial Questions shall help to establish a conversation, you might want to use these initial questions, but maybe you need to adjust your approach to other circumstances. After the initial questions you should continue with the topic that is most relevant for the person youôve recruited via an specific entry point (e.g. if an interviewee was recruited over the police start with topic 1) crime prevention)

Specific Entry point (Organisation, Venue, Event)	Random control group
-Why have you approached the organisation (*insert group specific organisation e.g. 1) Police, 2) Labour Unions, 3) Consumer Associations, 4) NGOs)?* -What were your concerns with ____ *(insert topic 1) crime prevention, 2) workplace surveillance, 3) consumer advocacy, 4) data protection)* -How did you come to know of the services offered? -What do you think about the activities of the organisation? *(insert specific one). Please explain what they do and how they can help you?* -Do you think your concern is something that is common or just a single issue? *-if more common: Explain and give examples* *-if singe issue: Why do you think other people do not experience this problem?*	*When interviewing a participant recruited randomly please start with the questions from one of the four major topics (Topic 1: crime prevention, Topic 2: workplace surveillance, Topic 3: consumer advocacy or Topic 4: Data protection).*

General Questions: Surveillance, Privacy and Control

a. Do you know places in your city where CCTV is operating?
b. What do you think about the use of CCTV in public space?
c. What do you think about the use of CCTV in private spaces?
d. What do you think is happening to the CCTV footage?

e. What kind of measure should be allowed to prevent crime?
f. What kind of measures should be allowed in order to catch criminals? Face recognition software, public photos of wanted persons (also online)).

g. What do you know about Drones or UAVs? Are those operated by the state, by private companies or by law enforcement authorities?

h. If you could decide: Which kind of persons or what kind of places should be monitored more frequently? Where should CCTV never be allowed to be used (and by whom)?

i. What do you think, in society did we experienced an increase or a decrease in the use of surveillance technologies over the past few years.

j. Have you ever heard about data retention, what is your opinion towards data retention?

Topic 1: Crime prevention	a1. Roughly speaking: In general would you say that the life in the city you are living has become more or less secure over the past few years? a2. What do you think, how many burglaries have been attempted in the last year in your city/village and how many violent offences have been reported to the police? --- b1. What measures have you personally taken to prevent crime (maybe specify: personal, house, burglary etc.?) b2. What can you imagine to install to protect burglaries? b3. Do you talk with your neighbours about these issues *(or orient yourself at your neighbours activities in this matter)?* b4. Do you and your neighbours take turns in watching over each others house/apartment? b5. Did you ever think about neighbourhood watch? If so --> why and with what result? If not ->> what do you think of it? b6. Besides practical measures that you take (may they be of technical or organisational nature) does this topic have an impact on your own behaviour (to you avoid certain locations at certain times) -> *If people do not take any measures to protect themselves than only ask the 2nd part of this question* --- c1. ñIf you play with fire, you must expect to get your fingers burnedò What do you think in connection with crime prevention about this saying? *(This questions is intended to check whether people feel* ***ñ****it is ok****ò*** *to take* ***ñ****hard measures****ò*** *against criminals or not, even for* ***ñ****minor****ò*** *offences like burglary)* c2. Is security an issue that one should take care about him/herself? c2. How far is this (c1) true for your sphere of personal privacy (your home for example) and how far for public places like cinemas, shopping malls, the street etc.

Topic 2: Workplace surveillance	a1. What forms of workplace surveillance do you know? a2. Which do you find acceptable? --- b1. Which forms of workplace surveillance have you experienced yourself? b2. At your workplace, do they use any time tracking applications? (Considering also ñlow-techò measures like a attendance time clock) b3. Can you understand why these measures were implemented? b4. Do you think these measures/systems infringe on your rights as an employee? b5. Has any control measures affected your work? - How? b6. Has any control measure affected your relation to your colleagues? How? --- c1. ñTrust is good, control is betterò In the context of modern working environment what do you think about this old saying? c.2. What do you think about human resources departments collecting information about applicants on social networks (like Facebook, Twitter, etc.)

Topic 4: Data protection	a1. When you are thinking about the ñdata protectionò what are the five terms/buzzwords that you think of first? a2. Did you ever experience problems with your own data, misuse or false accusations? Or do you know somebody who has experienced these kind of problems? b1. Do you use social networks, social media like Facebook, Twitter, Instagram etc.)? What kind of content do you share on these platforms? (Photos, Personal information, etc.) b2. How do you choose what parts of your life you share online (like avoiding political debates on Facebook, or not sending private photos via e-mail or sharing them on social media networks/platforms, or sharing photos of your kids/family with persons you hardly donôt know in ñreal lifeò). b3. Do you use cloud computing services like: iCloud, Dropbox, GoogleDrive, Mega? b4. How do you protect your (personal) data? (e.g. anti-virus software, firewalls, etc.) b5. Have you ever heard about any data protection authorities in your country? b6. What do you know about the work of a DPA? Do you know the national data protection officer by name? c1. Do you think that the general public is (well) informed about this topic? If not, why?
Topic 3: Consumer advocacy	b1. Do you own a loyalty card? If so, why? How many? Do you use them often? If not, why not? b2. How do these cards work? What kind of benefits can consumers gain from the use of loyalty cards? What kind of benefits do companies gain from these cards? Do you know about any negative effects these cards might have for consumers? b4. What data is collected through such technologies, e.g. loyalty cards or else? What kind of data is collected from the loyalty cards that you are using frequently? b5. Where do you see the dangers behind such collections? b7. Do consumers have a chance to resist? How? b8. What do you know in this respect about the work of consumer protection authorities? b9. Which shops do you visit frequently? Do these shops use CCTV? Do you know whatôs happening with the pictures/videos taken with CCTV? b10. E-Commerce: Do you regularly buy something over the internet? What kind of shops, sites do you visit frequently for shopping purposes? Ebay? Amazon? Which method of payment do you choose regularly when you shop online? What data is collected while you are shopping online? b11. Which e-mail provider do you use mostly? (Gmail, GMX, Yahoo Mail etc.?) Do you write/read your mails on- or offline? Which search engine do you use primarily? b13. Have you ever heard about target marketing? Do you know anything about the legal regulations regarding target marketing? --- c1. Have you ever heard about the term ñglass costumer or transparent costumerò? What do you mean by this? (for example: do you think it is in general problematic, that companies want to know as much as possible about their costumers?)

9.2.2 Guideline to synchronise data entry and coding

Regina Berglez

This compendium (of the essentially more detailed indication used within the process) is meant to illustrate how we actually transferred the órawô interview data (that consisted of taped records condensed into interview protocols) in a next step into our extensive database.

1. Question

Insert the actual question that you asked the interviewee:

1. If it was indeed an open general question, the following form is sufficient:
   ñ*General question on opinion on CCTV****ò***
2. Otherwise specify in brief what/how you asked:
   ñ*What do you think about the use of CCTV in public space? **ñ***
3. And if you dig deeper into the context, again, specify briefly what you referred to:
   ñ*And just going back to George Orwell, the 1984 thing, what do you mean by that?****ò***
4. If the greater context would otherwise be lost, you can insert an additional hint in brackets:
   ñ*Are you security conscious?****ò*** *(= this is in reference to having had an e-mail account hacked and a bank card skimmed on more than one occasion)*

Donôt indicate the topic without any further context e.g. ***ñ****crime prevention****ò*** or ***ñ****surveillance practises and methods****ò***.

2. Quote

Insert the translated story (=story/quote/statement)

1. Whenever possible, insert in the interviewees first person narrative:
   ñ*I think you canôt live nowadays without leaving some traces unless you withdraw from society and become a recluse in the forests. What people should not do is to leave more traces than necessary. I am thinking of Twitter, Facebook and so on. Thatôs because I simply think many young people that leave traces **ï** by doing fun things - nowadays will regret that in 5 or 10 years because the traces persist, because they [the traces] might cause damage.****ò***

Or ï in case it becomes complicated to insert the first person narrative ï you can also paraphrase in third person:

ñ*First, he said no. Then the participant remembered an experience from when he was visiting his parents in the countryside. After his mother told him several times about a sneaking thief who prowls around at his parents place, the participant lurked for the thief one night. Franz actually saw a stranger prowling around on their property that night****é*** *.****ò***

However, the first person narrative is the preferred option in order to catch phrases and other specifics (compare next point) and will also simplify decisions on the role/s of the storyteller later on.

2. Translate as verbatim as possible and necessary to grasp the content as well as specifics (e.g. irony, jokes, country-specific references):
   Especially if you have chosen to paraphrase the story (compare point 1 above) make sure these specifics donôt get lost in the process.
   ñé *Yes, and for instance since I know that Google is storing everything, everything can be tracked and found **ï** well, I do not need to google Hitler all the time **ï** but (excursus about the book **ñ**Mein Kampf****ò*** *and what a horrible botch it is) I was curious if this book is available nowadays, so I googled that - and then I said to my friend, in jest, **ñ**Now they will think Iôm a right-wing extremist****ò***. *Why arenôt I allowed to gain information without having ulterior motives, staying unmolested?****ò***
3. If necessary, insert an explanation [references/context/hint on excursus] in brackets:

ĂBack then [i.e. student milieu of the 70ies in Vienna], the personal freedom was at stake, personal freedom implies that you are not surveilled all the time, that I am not a model (é) there were a lot of fundamental rights that vanished after September 11th at the latest.ò

4. One story at a time; never insert the whole course of your conversation.
   We are going for *condensed* stories not for full transcriptions (compare underneath).
   Donôt: *ñIE No, I havenôt, really. No. I suppose weôre getting onto this, but I just accept that thereôs no privacy.*
   IV Okay, thatôs interesting.

5. There is no need for an exact transcription (pauses, filler words, repetitions etc.)

We are planning for a database consisting of a great number of stories

- ŏ which should grasp the original *content* (given the fact that they are to be translated ï in most cases ï into another language),
- ŏ within the translation process it is important to mind specifics (e.g. irony) since that is important information for the later analysis,
- ŏ but we are not going to conduct any depth interview analysis or the like,
  hence the wording/quotes can and should be condensed to what is to be seen as a story at a time (as in the given examples).

3. Paraphrase

Now you summarize the story:

1. in short
2. as a stand-alone (understandable without any other context)
3. grasping the core proposition
4. written in third person
5. but without (your) interpretation.

Good practise examples:

ñThe storyteller complains about the lack of privacy and personal freedom when he moves on public places in Vienna or travels in the UK or US. He compares the circumstances to a dystopian novel by George Orwell.ò

ñThe participant reports an annoying security measure at a small American airport. He claims that social sorting happens at airport controls.ñ

ñRespondent reflects on the pros and cons of loyalty cards. Raises ecological concerns. On the other hand he admits at the same time being receptive to the offers.ò

Donôt: ñCrime prevention and neighbourhood watch in a small townò (no proposition)
ñYou could resist but it would be probably pointlessò (no context, still verbatim)

4- Type of the Story

Descriptive narrative:
This is about a ŏreal life storyô that had actually happened to the storyteller, to a friend of the storyteller or is referring closely to a real story that has been on the news etc.)

ñI remember a car theft. It happened to a good friend in Praha. It probably was in the early 90ies. He worked thereé é ò

ñ*Yes, in fact it was a conversation I'd had with the .... County Council and I'd felt that I'd been treated in a bad way on the phone and I wanted a recording of the conversation****é ò***

Normative account:
This is about opinions, beliefs, theories etc. about society, surveillance, utopiaé .

ò*I think you can't live nowadays without leaving some traces unless you withdraw from society and become a recluse in the forests. What people should not do is to leave more traces than necessary****é .ò***

ñó*The participant thinks that it is important to inform the society. He thinks there was a phase in which the society was informed sufficiently via the media [news]. But that was only a phase****é ò***

5. Setting of the Story

If a "real life story" was told (=had happened to the storyteller, to a friend of the storyteller, referring closely to a real life story on the news etc.):

Insert the actual *place* and (if possible) date of the story*:*
ñA small town between Milan and Turinò (in 2012)
ñThe storytellers flat in Viennaò (in the 1990s)

Or even ï if possible ï more detailed:
ñThe city of Prague in the early 90s at the end of the communist area in east/central Europe.ò

If it was about opinions, beliefs etc. the wider *topic* becomes the setting of the story, please insert, (if possible with information on the timeframe etc.):
ñAir traveling in modern times.ò
ñUse of social media after Snowdenò

Or even / if that abstract:
ÄLiving in a surveillance societyò
ñDescribing Utopia, where as the investment in human beings solves general problems.ò

Don't ñthe Internetò (too wide, non-specific)
ñInterview with member of NGO groupò (=This is general interview information -> either referring to the recruiting topic and/or general information at the very end)

Please remember to avoid cross-references between individual text input fields. Ideally every single entry should make sense without further context.

Please note that all questions following from now on are referring to the ROLE OF THE STORYTELLER only in every very PARTICUAR story.

6. ROLE OF THE STORYTELLER - Knowledge:

Expert: S/he is speaking from an informed position
ñ*I know where the cameras are here and they are not effective in terms of security. For instance, here local police patrolling the streets has been much more effective for bags snatching. This is prevention, not CCTV that can be useful only after something has occurred.*

Lay: S/he is speaking from a less informed position
ñ*Until now, I haven't found a reason why I should say: hey, this [data protection] is of real importance for me. Because I'm generally the opinion, that everything I do, if I'm leading a good life, that everything I do should be representable****é òò***

7. ROLE OF THE STORYTELLER - Role:

Most of the times the categories should be adequate, however, if in a normative story the role is impossible to determine, please tick the option Normative account

Watcher: *ñI have worked for the federal ministry for agriculture and forestry and I have been a system administrator there. We knew exactly when somebody turned on a computer, what program he started first, that was all [accessible for us]é ò*

Watched: ñ*In principal, you have become almost hundred percent transparent (glass citizen)ò*

Detached observer: *ñIn a time in which especially young people reveal everything ï beginning with credit cards to some kind of striptease that they put on Facebook ï one must not be surprised when everything is in some way public or publishable. Iôve never bought something on E-bay or Amazon but not because I am afraid of such things but simply because it is not my medium. é ò*

Active observer: *ĂIf I want to participate, I need to be willing to expose certain parts of my personal data. I myself determine where I disclose which datae ò*

8. ROLE OF THE STORYTELLER ï Level of attitude: e.g.

Pro: *ñTo be honest, I donât have any objections. When something happens, like stealing, then you can more or less immediately chase him [the thief] when a video surveillance is existent. I would not mind it at allé ò*

Contra: ñ*I think my daughter is on Facebook, but I think that is the only one [social media site]. For me it is absolutely uninteresting, a waste of time, very roughly speaking. (é) what data protection meant in the 70ies, what disappeared in the last 30 years, and how you have become transparent [ñglass citizenò] nowadays is in principle a catastrophe.ò*

Uninformed: *ñI think the main reason is that young people are very keen on expressing themselves. I donât know. Iôve been told é ò*

Ambivalent: *ñActually itôs hard to understand for me, but Iâll try, but I donât have to participate on Facebook. Of course itôs fascinating what you can find there. Iôm a curious person you know. I like to know something about other people. For example about former schoolmates.ò*

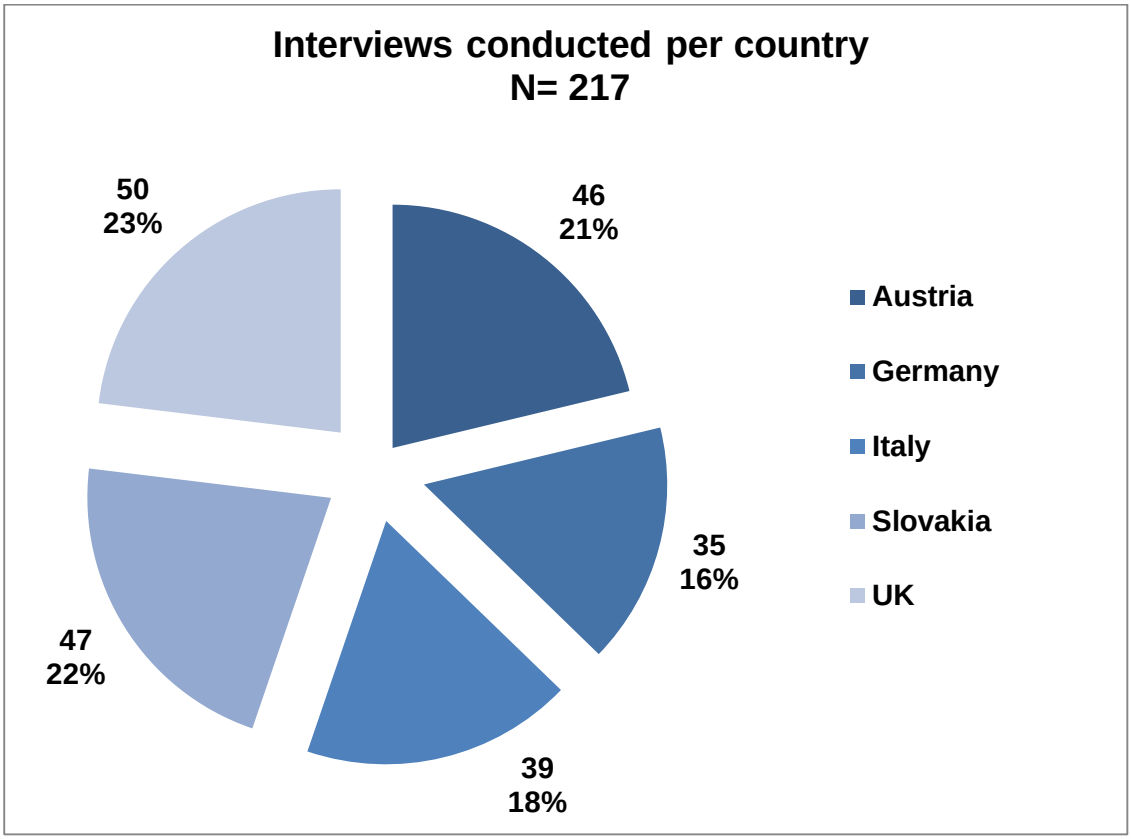
9. ROLE OF THE STORYTELLER ï Level of action:

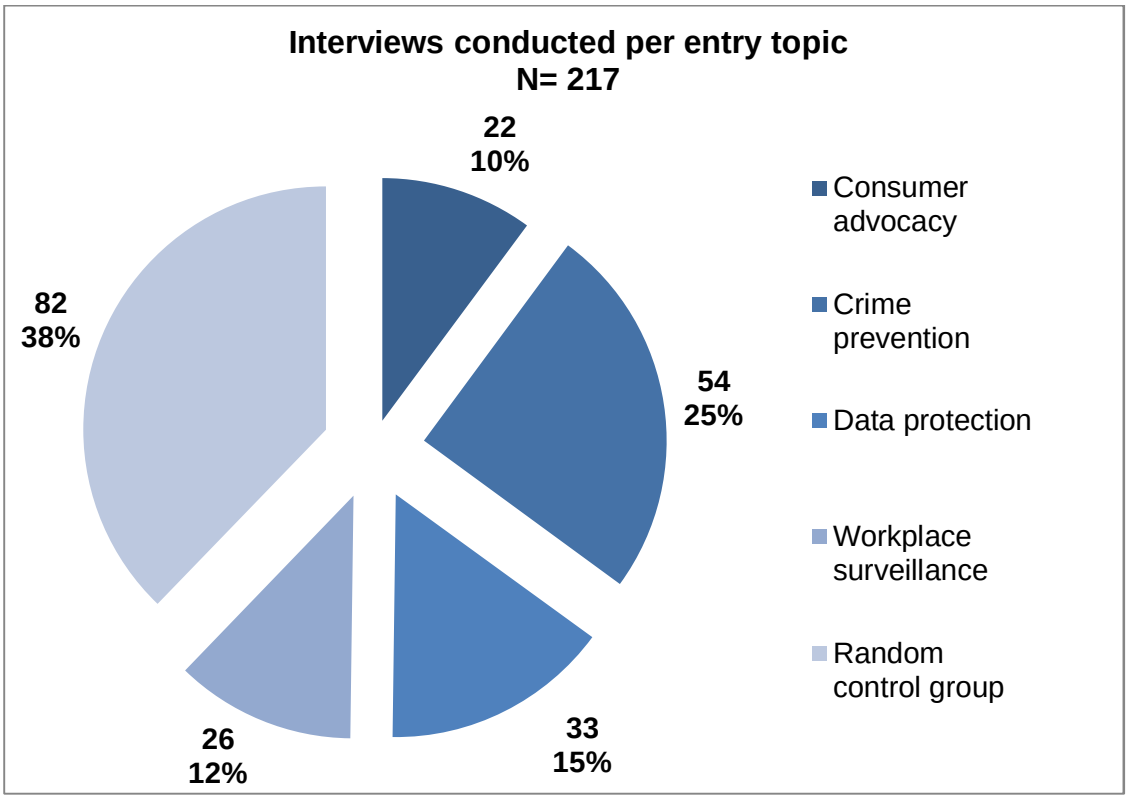
Active: *ñLast week on the radio there was a speaker talking about big companies that usually have a psychologist to manage the interview for selecting candidates and they also check the FB profile of the potential candidate, although I havenât a big company, I agree with this system for profiling the person you are going to interview and potentially employé ò*

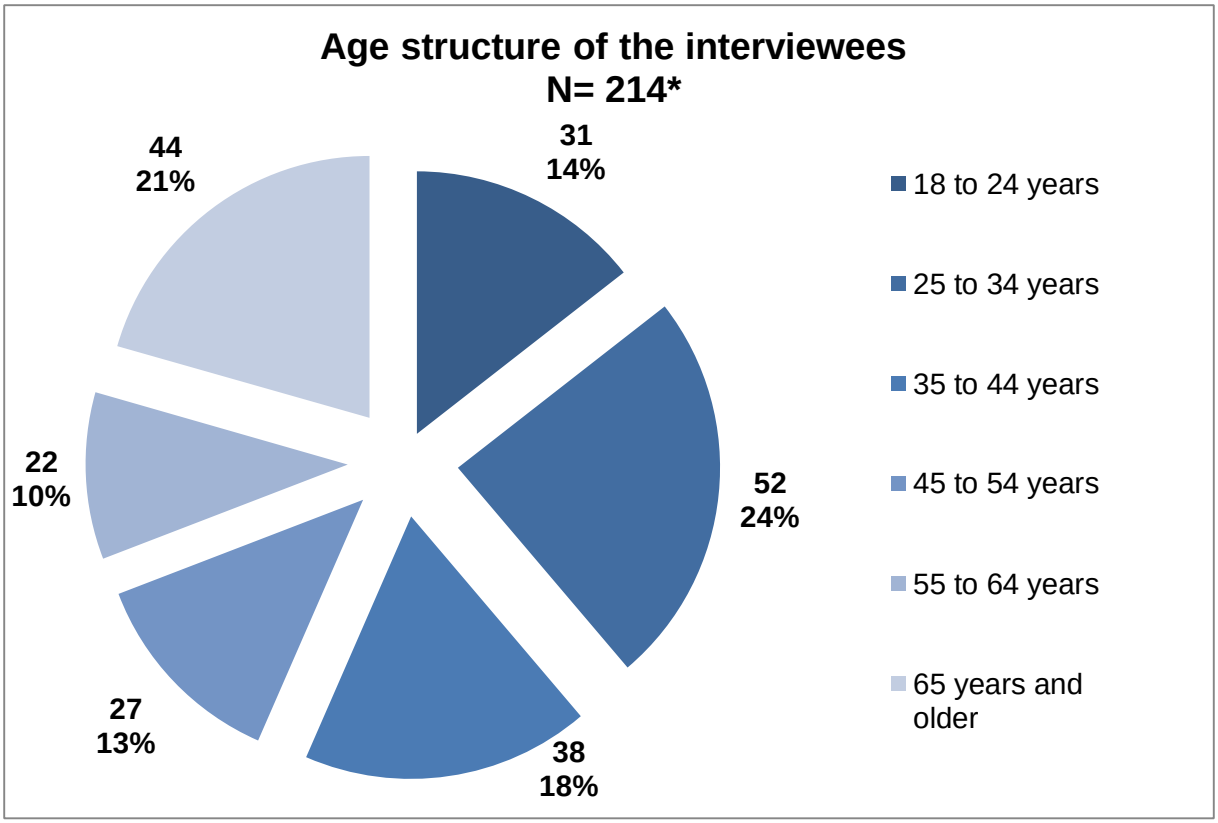
Passive: *ñI am not one who is aware of a lot of things [in the neighbourhood]. I know at most who lives in the houses. But we have one [guy] in the first house of the street who knows everything. There is nothing he is not aware ofé ò*

9.2.3 Overview on the conducted interviews and interviewees

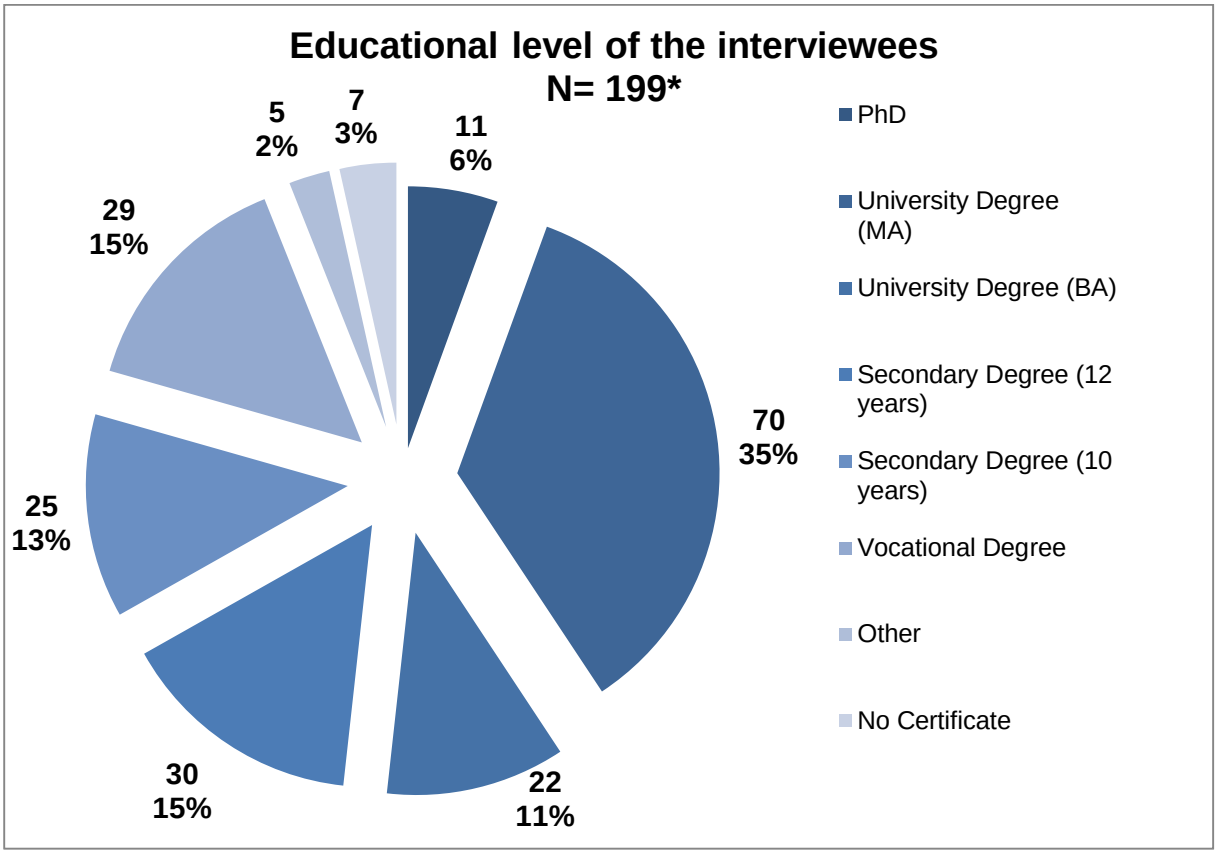
Regina Berglez



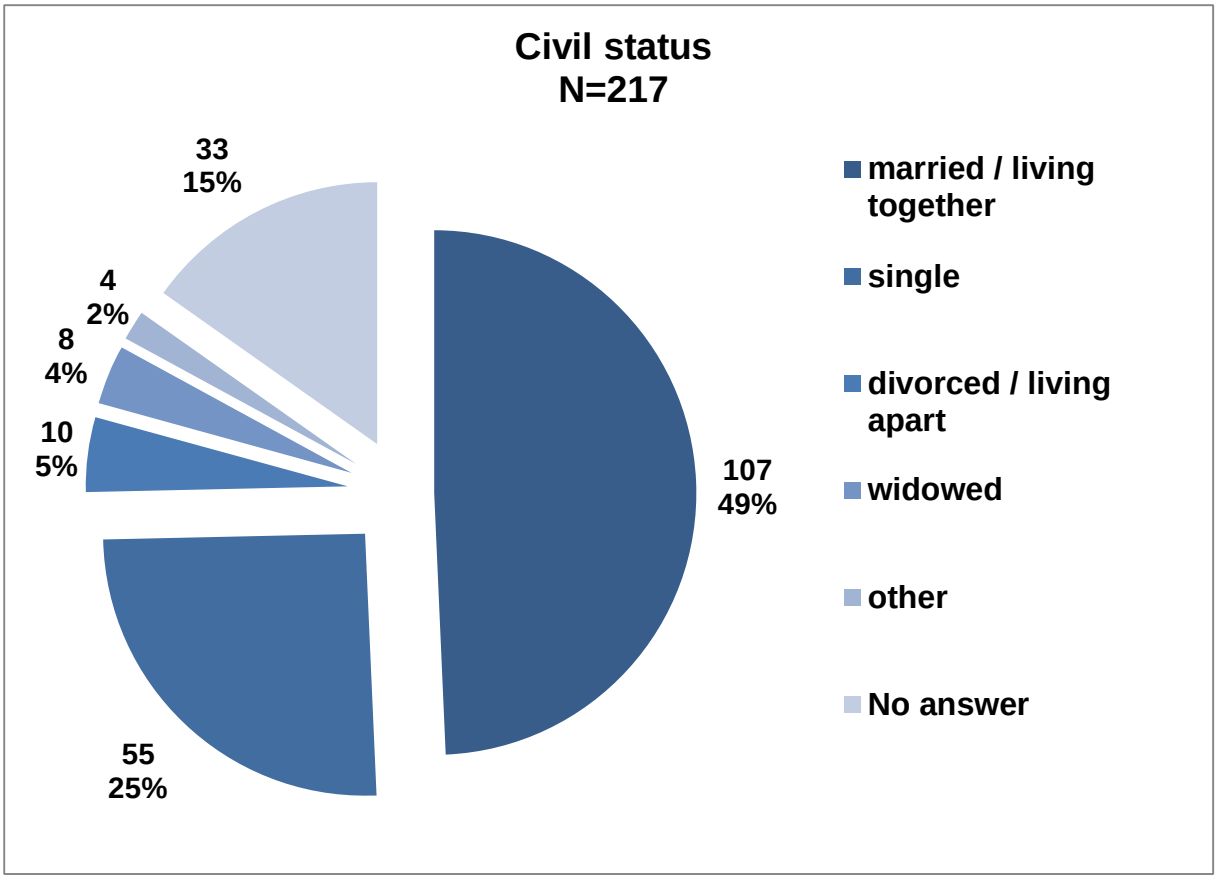


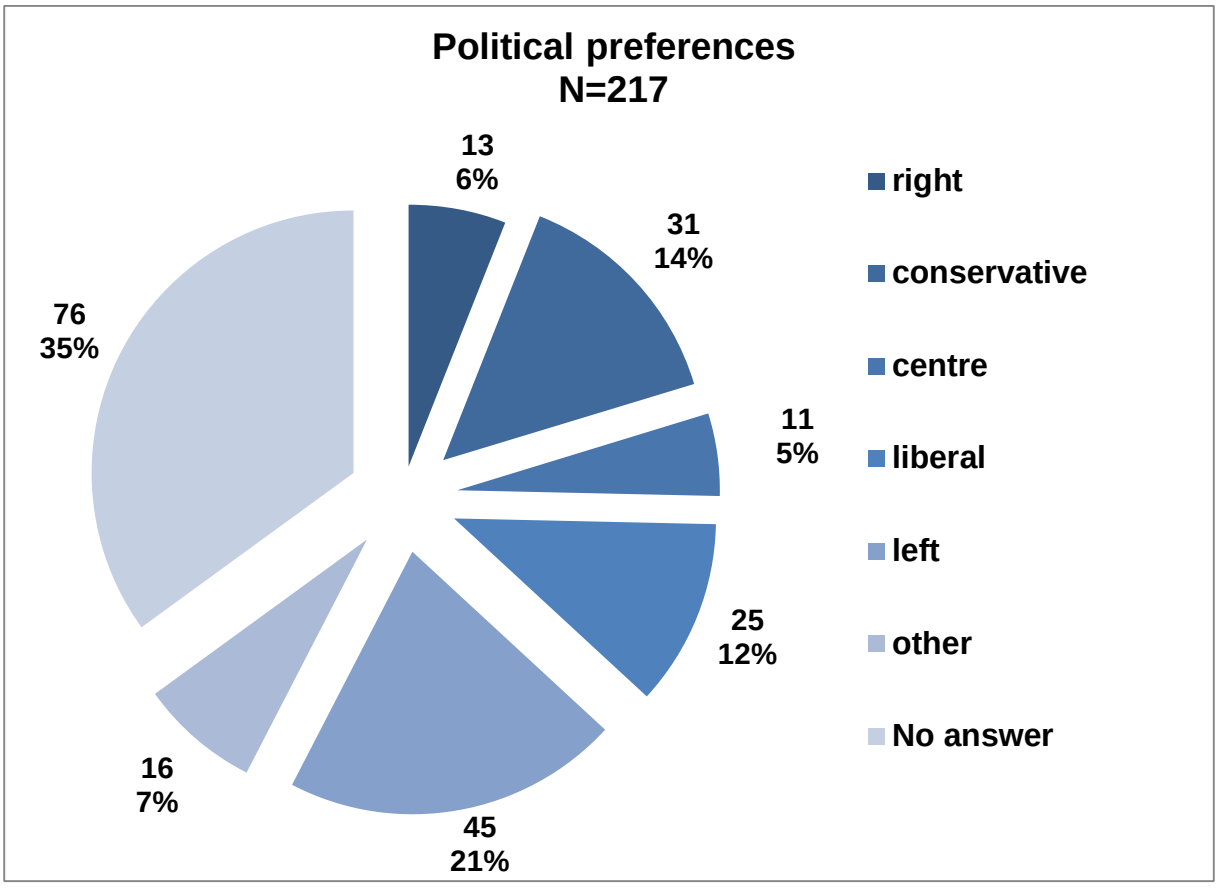


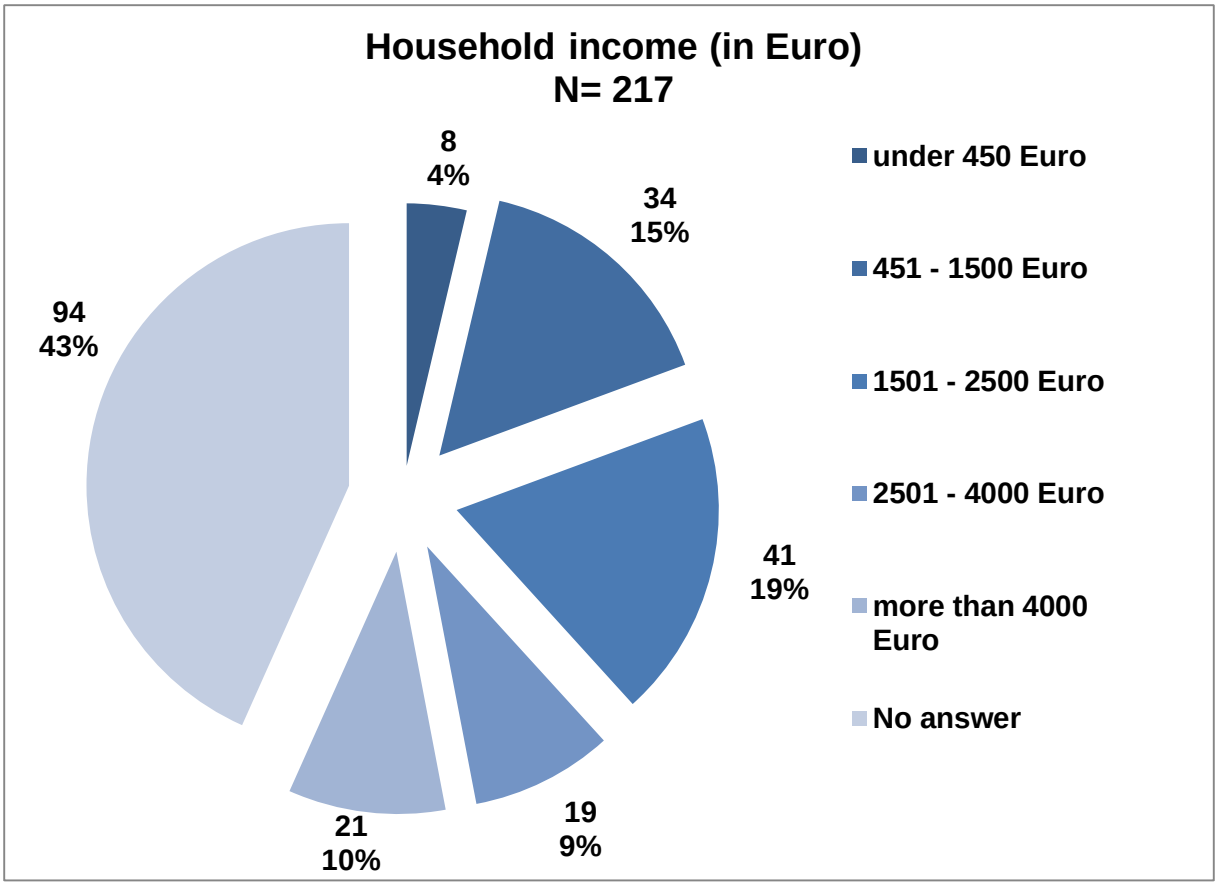
- 3 missing

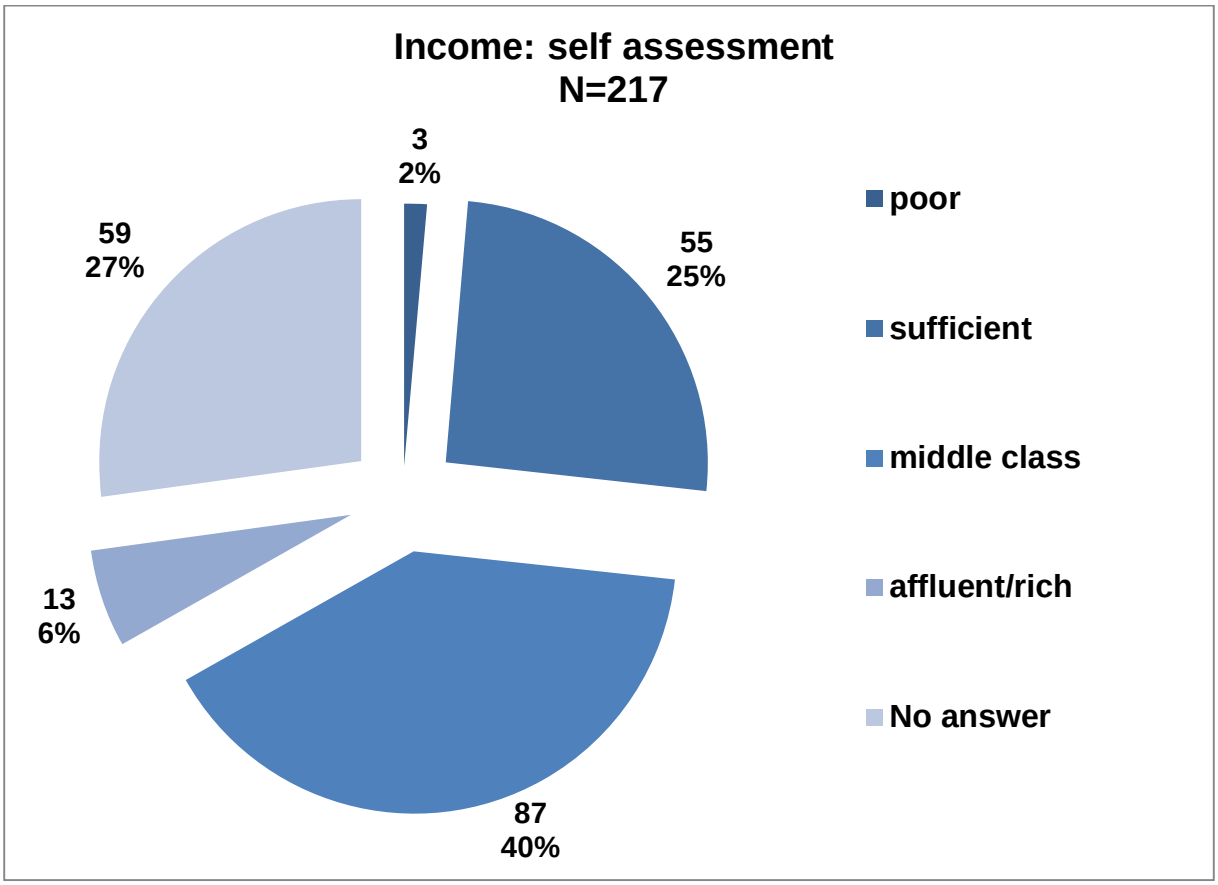


*18 missing


Civil status
N=217
33
15%
4
2%
8
4%
10
5%
107
49%
55
25%
married / living together
single
divorced / living apart
widowed
other
No answer


Political preferences
N=217
13
6%
31
14%
11
5%
25
12%
45
21%
16
7%
76
35%
right
conservative
centre
liberal
left
other
No answer


Household income (in Euro)
N= 217
8
4%
34
15%
41
19%
19
9%
21
10%
94
43%
under 450 Euro
451 - 1500 Euro
1501 - 2500 Euro
2501 - 4000 Euro
more than 4000 Euro
No answer


Income: self assessment
N=217
3
2%
55
25%
87
40%
13
6%
59
27%
poor
sufficient
middle class
affluent/rich
No answer

9.3 ANNEX III ï FOCUS GROUPS HANDBOOK: IRISS TASK 4.3

Walter Peissl

9.3.1 Introduction and Methodological Background

The objective of this paper is i) to present the methodological background and aims of Focus Groups (FG) within the framework of IRISS WP4 and ii) to provide concrete organisational guidelines for conducting the FG within Task 4.3 ñInformed Debate on Surveillance and Controlò.

The FG roots in experiments and experiences of American Sociology in the late 40ies of the 20th Century. Robert Merton together with Patricia Kendall (1946) published a fundamental article about ñThe Focused Interviewò, which is deemed to be the ñlandmark paperò of this method. They based their findings on several years of experiences in studies of social and psychological effects of mass communications. Since then hundreds of thousands of FG have been conducted all over the world and a bulk of literature on the method was written. FG meanwhile is widely used and developed professionally.

Definition

Besides the above-presented US American development there was a parallel one in Germany. ñGruppendiskussionò/Group discussions were used in the 1950ies for researching political awareness of the Nazi past (Dürrenberger/Behringer 1999). From these different strands a variety of definitions evolved. They all have in common, that a Focus Group is a moderated group discussion, on a specific issue and used to research attitudes and values. Some of the definitions vary in the size of the groups, the amount of meetings and other details. A pragmatic all encompassing definition, which is working for IRISS too is given by Steyaert/Lisoir (2005): òA focus group is a planned discussion among a small group (4-12 persons) of stakeholders facilitated by a skilled moderator. It is designed to obtain information about (various) peopleôs preferences and values pertaining to a defined topic and why these are held, by observing the structured discussion of an interactive group in a permissive, non-threatening environment. Thus, a focus group can be seen as a combination between a focused interview and a discussion group.ñ

Applications

FG are mostly used in commercial marketing research for testing new products. In the 1980ies FG entered the arena of policy advice ï testing political campaigns and programmes, medical planning ï discussing health policy programmes and more generally the qualitative social sciences ï investigating attitudes, preferences and values.

Principles

Summing up: a FG basicallyé

- consists of 4-12 people,
- needs a stimulus for triggering the discussion,
- is a moderated discussion,
- that needs an open climate and
- is non-directive.

The Focus Groups in IRISS

One of the objectives of IRISS is to understand and reconstruct citizensô views and understanding of surveillance and their options to exercise their democratic rights in surveillance societies. WP 4 is devoted to these citizenôs views and attitudes. Based on the experiences from former tasks in WP 4 it is the overall aim of task 4.3 to investigate whether there are differences of attitudes and lines of

argumentation towards surveillance and control ñbeforeò and ñafterò having reflected on the issue. Therefore task 4.3 will recruit their subjects partly from the pool of respondents/participants established in task 4.2 (already in touch with the issue) and partly new participants who have not been in contact with the issue at stake/the project before (ñControl Group IIò). These FG will be held in 5 partner countries: Germany, Italy, Slovakia, the UK and Austria.
The ñinformed debatesò are focus group like moderated group discussions. The events will be recorded and partly transcribed. The goal of these focus groups is to gain a deeper understanding of the attitudes and opinions held by different groups of citizens in different countries and to test the stability of these opinions and attitudes when confronted with new information. By involving citizens in such an informed debate, we will be able to better understand how surveillance resonates with societal values held by different groups.

9.3.2 Organisational Guidelines

Before the FG - In short: what, who, when and where?

What?
In IRISS we are conducting a classical FG with introductory stimulus, provided by the moderator in the beginning. The introductory material (cases/quotes based on the database of the interviews round 1 and 2) will be provided in English and has to be translated by partners in their respective language.

Who?

- Partners/organisers need a task leader, taking care of the whole process including recruitment, other organisational issues and the analysis. For the FG partners need at least two staffers: a moderator, leading the discussion in a non-directive way and an assistant, taking care of the technical stuff (recorders, paper, pens etc.) and supporting the moderator where ever necessary. In IRISS weôve reserved 1,100 EUR extra budget (other direct costs) to cover the expenses of the FG.
- The participants shall come from two different sources: ñreflectedò from interview round 1 and newly recruited ñnewbiesò. For details see 3.1.2 below.
- In countries with more partners involved, the focus groups will be split between the partners with shared responsibilities (possibly one focus group conducted by each partner).

When?
The event shall be organised subsequent to the in-depth interviews of task 4.2 and will take about 2 hours each. This actually means that the FGs should take place in January-February 2014. In order to do so recruitment may start immediately before/after Christmas. Start recruiting 2 weeks before the envisaged date at the latest! You can find details in 3.4 Timeline.

How long?
Each FG has an average duration of 2-3 hours maximum. This means you may conduct them in the late afternoon. Starting relatively late may attract people to come, because they donôt have to get off work too early. Schedule the FG according to your countries habits (in Austria we intend to go for Monday 17:00).

Where?
The venue should be an open, friendly, central place, which is easy to reach and big enough for a group of 10-12 people sitting around a table or in a circle. Especially important is that the venue is not manipulating. With regard to the issue at stake you should not conduct the FG in the Ministry of the Interior or at the premises of Privacy Advocacy NGOs etc.

WP4 Sampling overview

It is aimed for two focus groups per country. The participants of both groups are by no means representative but a good mix with regard to socio-demographic factors (gender, age, education etc.) shall be aimed at.

The table below shows the ideal sampling in all activities in WP4. With regard to Task 4.3 the last row is relevant. Partners should aim at finding two groups as similar as possible to the participants from round 1. Main criterion is still the ñentry pointò, which means participants should be recruited according to the list below. Secondary criteria with respect to similarity to the first round groups are socio-demographic variables as far as they played a role in the first round interviews. This means each partner should try to find as many male/female participants as in the first round interviews for both the ñreflectedò and the ñnewbieò group in their respective country. The same goes for equally distributed age samples and so on.

Always bear in mind: try to come up with two groups as similar as possible to the participants in interview round 1, because the main objective of Task 4.3 is to find out whether there are differences between those already reflecting about surveillance and control and those who havenôt so far.

Recruiting strategies

For the ñreflectedò participants please have a look at your database and try to get in contact again with the interviewees and just ask whether or not they are willing to join a Focus Group. As soon as you obtain informal acceptance you may send a more formal personalised invitation letter (probably via mail/pdf attachment) with all the formalities (see Appendix). Basically you will know how the group will be best composed, as you know the people from the interviews. Try to make the group as different, interesting as possible.

For the newbies just go ahead and try to find your ñControl Groupò participants out there at random. You may use your institutions website, Twitter, Social Media Platforms or classical telephone book like recruiting strategies. You can use a slightly changed ñInvitation letterò for the broad advertising of the Focus Group events. Probably you may get more positive responses than you need participants (8-10), so you have to select according to the targeted portfolio.

The moderator should not know participants and participants should not know each other. This counts for both groups.

During the FG

Introductory input/stimulus

In the beginning of any Focus Group you have to open up the field and give a short introduction to the issue at stake. This should rather be a short 5-10 minutes opening talk, not a comprehensive presentation. In the IRISS case we decided to take advantage of the international attention surveillance received through the disclosure by Edward Snowden. In order to introduce the issue we need a common language, but not necessary the exact same words. The following text is a kind of structured basket of modules that may be used by the facilitators according to their national needs.

Besides the common definitions, explanations we also provide the participants with some potential reactions to the global surveillance scandal. In order to do so we looked at the IRISS database from the interviews and would like you to use some of the following quotes to illustrate attitudes that popped up during the interview series. Reactions to the Snowden/PRISM scandal ï the ñglobal surveillance disclosureò ï can be:

- Raised awareness
- Neutralising
- Ignoring
- Ascribe political relevance

In the introductory statement you should use quotes illustrating at least two of the above categories of potential reactions. Best would be to illustrate different kinds of reactions with most potential

difference: describe ñraised awarenessò by one quote and ñignoringò by another; or use a quote for ñneutralising strategyò and another for ñascribing political relevanceò. If you can come up with quotes for all categories it would be best. The more open the field for discussion is, the better, but be aware of not being too long with the introductory statement. The quotes are a kind of basic material to be used in your introductory statement ï use one or a combination of two, just try to sketch a broad picture of possible ways to cope with the situation.
With the quotes (see below) you will see from which country they are ï if one of your participants in the ñreflectedò FG is the source of a respective quote you shall not use this one and take another instead. For easier comparison I would encourage you to use the same kind of introductory statement in both FG.

Definitions/wording:

The **ñ***global surveillance disclosure***ò** refers to an on-going series of news reports in the international media that revealed operational details regarding the U.S. National Security Agency (NSA) and its international partners' mass surveillance of foreign nationals as well as U.S. citizens. The vast majority of reports emanated from a cache of top-secret documents leaked by ex-NSA contractor Edward Snowden. On June 6, 2013, the first of Snowden's documents were published simultaneously by The Washington Post and The Guardian, attracting considerable public attention. In summary, these media reports have shed light on the implications of several secret treaties signed by members of the UKUSA Agreement in their efforts to implement global surveillance. For example, Der Spiegel revealed how the German Bundesnachrichtendienst (BND) transfers "massive amounts of intercepted data to the NSA", while Sveriges Television revealed that Sweden is continuously providing the NSA with data gathered from telecom cables intercepted by the FRA (Försvarets radioanstalt), under a secret treaty signed in 1954 for bilateral cooperation on surveillance.[369]
PRISM is a clandestine mass electronic surveillance data mining program known to have been operated by the United States National Security Agency (NSA) since 2007. PRISM is a government code name for a data-collection effort known officially by the SIGAD US-984XN. The Prism program collects stored Internet communications based on demands made to Internet companies such as Google Inc. under Section 702 of the FISA Amendments Act of 2008 to turn over any data that match court-approved search terms. The NSA can use these Prism requests to target communications that were encrypted when they travelled across the Internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier, and to get data that is easier to handle, among other things. Its existence was leaked 2013 by NSA contractor Edward Snowden, who warned that the extent of mass data collection was far greater than the public knew and included what he characterized as "dangerous" and "criminal" activities. The disclosures were published by The Guardian and The Washington Post on June 6, 2013. Subsequent documents have demonstrated a financial arrangement between NSA's Special Source Operations division (SSO) and PRISM partners in the region of millions of dollars.[370]

Quotes from WP4 interviews

Raised awareness

GER	*Since the Edward Snowden thing Iôm much more aware now that my location data could be accessed by the police if they wanted to access it but as Iôm not a criminal I donôt really mind that I suppose. ..... thereôs a huge amount of data on Google about me that if the*	Raised awareness: but nothing to hide, nothing to fear

[369] (https://en.wikipedia.org/wiki/Global_surveillance_disclosure (accessed 2013-12-17))
[370] (https://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29, accessed 2013-12-17)

	police could access it they could pretty much find out my whole life so, I was debating whether to delete it or not. Iôm not sure what to do yet because I then thought to myself, well as Iôm not a criminal itôs quite good that Iôve got my location data on there because if someone accused me of doing something I didnôt do then I can say, well, look, log into my Google account and you can see exactly where I was on this date or time, to prove that I wasnôt there. ... Itôs made me think more carefully about how much data they do store on me because Iôm just aware that all my searches Iôve ever done since 2006 probably will definitely impact on it, Iôve checked since the Edward Snowden thing.	
GER	*Yes we have Dropbox, only for professional reasons. And I must say: Even if the BND, the NSA or something gets this data: I don't care, this is no sensitive material, normal photos.*	Raised awareness: but nothing to hide, nothing to fear
AUT	*Yes, I donôt feel comfortable about it. But I donôt know what they actually should do é Itôs just a feeling when you put too much é You heard now a lot of all these scandals and so é Itôs just a bad feeling. I donôt think the government is spying on me or something like this é Itôs just that I think some things should be just private é private life é institutions shouldnôt have access to é Some things should be in the private sphere of individuals é not like in the US where everything is already monitored é like when they said, one week before é it was revealed that they (NSA, PRISM) check all the mail in the United States. Thatôs crazy because itôs a private part of the individual. I mean is it interesting to check all the post cards?*	Raised awareness
Neutralising		
AUT	*Hm no... I rely a bit on my partner, he's an IT-Nerd and very much into that data protection thing too. When he uses all the stuff, also for sensitive data, Dropbox, cloud, the same email-provider then why should I worry?*	Neutralising: Rely on partner/friend
GER	*No, I never believed that email-communication was a trustworthy, private, safe space. That "postcard"-metaphor, you know that everybody who's server is passed while sending the mail can read it... That's nothing new, I have friends working in the IT-Sector, they told me that years ago.*	Neutralising: nothing new
Ignoring		
AUT	*Honestly, I donôt fully get all these discomposure about the NSA-surveillance. That all these ócchecking everything out and collecting whatever is thereô especially on the internet is going on (quote interviewer ->he is deliberately? not using the term surveillance) was somehow clear for quite a while. What is possible to be peeked will somehow be peeked.*	Ignore: Nothing to do about it
GER	*I am permissive with lots of data. I talk about my income, because I DO NOT think money is so important. yes. I talk about sexual*	Ignore: Nothing to hide, nothing to

	preferences, not to everybody but yes among friends, because I DO NOT think it is so important. And if someone who I don't know and who doesn't know me reads this - I don't care.	fear

Ascribe political relevance

UK	*What I can say is that the Snowden type of problem is real. And the Googles and the commercial enterprises of this world are obliged by law to hand over comms data. But there's a difference that people need to get into their heads between common data which is traffic analysis, who's talking to whom or which device is talking to which device, that doesn't guarantee who is talking to whom, useful though that is, otherwise they wouldn't do it, but that in itself is not the same as reading communications. So there is a difference between the traffic analysis and the interception pieces. And I think people are quite rightly worried about the interception bit but sometimes construe the two aspects.*	Differentiate between commercial and state surveillance
AUT	*It's not strange, I get angry because people don't understand how important it is. Only yesterday I discussed this with a friend, and she said: Who cares if they read that I baked muffins today? And the point is: it is of interest. People just don't see that what they think is banal is still important enough to be recorded.*	Political Dimension: missing understanding for the importance of the NSA-case in the general public

9.3.3 Guiding questions: ñInformed Debate on Surveillance and Controlò

The guiding questions shall enable a free debate among participants on surveillance. By using the same template with both groups (informed/reflected and non-informed/newbies) and in all participating countries we will get inside into cultural/national peculiarities (as expected within task 4.2 as well) and additionally whether the participation in the interview round one has influences on attitudes on surveillance.
Questions in bold are supposed to be discussed by the participants. Subsequent to every question is a short note on the purpose of the question.
To most of the questions there are some subordinated questions. These subordinated questions are inspirational, and can be used to support the discussion if necessary. The subordinated questions do not have to be raised if it is not necessary to inspire the debate.
The question list below provides a flexible structure. So be aware of tackling all questions but not necessarily in the order provided here. Rather follow the group discussions own conversation process.

1) What are your immediate thoughts about the stories heard?
Purpose of the question: An open question to get the debate started and to give the participants the chance to present their immediate attitudes
Subordinated question to inspire the debate ï only if necessary:
- What were the messages of the stories?

2) What do you think about surveillance in general?
Purpose of the question: An open question to get the debate focussed towards the issue at stake

Subordinated question to inspire the debate ï only if necessary:
- What kind of surveillance do you know ï try to give some examples?

3) What do you think are important positive potentials of surveillance?
Purpose of the question: Make the participants focus on the positive potentials and get an impression of what they find is the most important gain of surveillance
Subordinated questions to inspire the debate ï only if necessary:
- What can you gain with surveillance ï try to give some examples?
- What is the most important positive possibility?
- Why is it important?

4) What do you think are important negative potentials of surveillance?
Purpose of the question: Make the participants focus on the negative side of surveillance, the threats, and get an impression of what they find is the biggest threat
Subordinated questions to inspire the debate ï only if necessary:
- What negative effects of surveillance ï try to give examples?
- What is the most important negative effect of surveillance?
- Why is it important?

5) Do you see any difference in surveillance by public authorities or by private entities?
Purpose of the question: To get the participants input on potentially different attitudes towards public or private surveillance
Subordinated questions to inspire the debate ï only if necessary:
- What kind of public surveillance do you know ï try to give examples?
- What kind of private surveillance do you know ï try to give examples?

6) Who should be involved when deciding on implementing new surveillance measures?
Purpose of the question: To get the participants input on the democratic perspective and importance of involving different interest groups when deciding on implementing new surveillance measures
Subordinated questions to inspire the debate ï only if necessary:
- Which interest groups should be heard? (Citizens in general, civil rights organizations, security technology developers, politicians etc.)

7) Do you have any suggestions about the regulation of implementation of surveillance measures?
Purpose of the question: To get the participants input on how to manage development and implementation of surveillance measures
Subordinated questions to inspire the debate ï only if necessary:
- Should governments implement every surveillance measure they find important or should there be some regulations ï and if so what regulations?

8) Has your participation in todayôs event changed your attitude towards surveillance? If so: Why?
Purpose of the question: To find out if information and debate about surveillance, security technologies and privacy have changed the participants attitudes toward the subject

9) Do you have any final remarks, points or messages that you would like to add? (take a round)
Purpose of the question: To give the participants a change to make a last statement before ending the interview meeting

Subordinated question to inspire the debate ï only if necessary:
- Have something made a special impression on you during the conversation?

Rules of thumb
These chapter provides you with some ñRules of thumbò and tips on how to carry out the FG in a good way.

Introduction
Start by presenting yourself, òMy name is é Iôm from é , and Iôm going to be the moderator at this group conversation. But you just talk and I will make a list of speakers if necessary.

After that you do a presentation round where people say their name and why they have come to the FG

After that the TAPE RECORDER IS STARTED !! This is done in a free-and-easy way and by an easy comment. It is important to create a light atmosphere and play down the seriousness to make sure that the participants are not oppressed by the situation.
The first question is raised and the FG is on its way.
The first question is always a ñbrainstormò question, and a can affect a lot of immediate attitudes. It is important to give space, be open and listen in the beginning.

On the way
It is not important that all participants answer all questions, but the interviewer should have an impression of what they all think.
If anyone is hiding, the interviewer can always ask ñDo you agree, John, or what do you think?ò

There will be overlap in questions and answers. Skip questions if they have already been debated and answered
Tick off on the way, when you think that a question have been debated

It is important that all questions are debated. But questions that are more important to the participants than the ones in the interview guide can appear in the discussion and there should always be time to discuss these questions (as long as they are related to the security and privacy debate).

If someone becomes too dominating, it is the moderatorsô job to bring on the other participants. Ask e.g. òWhat do the rest of you think?ò Interrupt if necessary, it is important that everybody is heard.

If the participants donôt say much at the FG, the moderator can ñtake a roundò saying that ñat the next question I would like to take a round where everybody gives an answerò.

Ask for reasons and arguments, ñHow come you think thaté / What is the reason foré

Be aware of the participantsô reactions; do they feel comfortable, do they seem under pressure or uneasy etc.

If you are through all the questions before time, you can go back to some of the questions that have not been debated that much on the way.

Closing

When there is 7-8 minutes left, it is a good idea to take a round where everybody gets to make a final remark. The final remark can be things that they have not have the time to state already or points or messages they would like to underline.

You can also ask if something has made a special impression during the conversation.

After the FG

Analyses

- Discuss FG immediately after the FG with assistant(s).
- Write down immediate impressions, reminders etc.
- Listen to recordings.
- Write a short ĂCountry Report on FGñ (5-10 pages incl. material)
- Translate most important results, quotes, arguments etc.
- Send Country Report and English material to ITA.

9.4 ANNEX IV ï THE FOCUS GROUPS

Walter Peissl; Wolfgang Bonß, Alessia Ceresa, Daniel Fischer, Chiara Fonio, Martin Kovaniļ, Erik Láģtic, Charles Leleux, Keith Spiller

9.4.1 Introduction: Informed debate on surveillance and control

Walter Peissl

One of the objectives of IRISS is to understand and reconstruct citizensô views and understanding of surveillance and their options to exercise their democratic rights in surveillance societies. Based on the experiences from former tasks in WP 4 it is the overall aim of Task 4.3 to investigate whether there are differences of attitudes and lines of argumentation towards surveillance and control ñbeforeò and ñafterò having reflected on the issue. Therefore task 4.3 established a series of Focus Groups (FG), which recruited their subjects partly from the pool of respondents/participants already interviewed in Task 4.2 and new participants, who have not been in contact with the project before. The FG were held in 5 partner countries: Austria, Germany, Italy, Slovakia and the UK. The ñinformed debatesò were recorded and (partly) transcribed. The goal of these Focus Groups was to gain a deeper understanding of the attitudes and opinions held by different groups of citizens in different countries and to test the stability of these opinions and attitudes when confronted with new information.

Methodology[371]

The FG roots in experiments and experiences of American Sociology in the late 40ies of the 20th Century. Robert Merton and Patricia Kendall[372] published a fundamental article about ñThe Focused Interviewò, which is deemed to be the ñlandmark paperò of this method. They based their findings on several years of experience in studies of social and psychological effects of mass communication. Since then hundreds of thousands of FG have been conducted all over the world and a bulk of literature on the method has been written. Meanwhile the FG is widely used and developed professionally.

Besides the US American development presented above, there was a parallel one in Germany. ñGruppendiskussionò/Group discussions were used in the 1950ies for researching political awareness of the Nazi past[373]. From these different strands a variety of definitions evolved. They all have in common, that a Focus Group is a moderated group discussion, on a specific issue and used to research attitudes and values. Some of the definitions vary in the size of the groups, the amount of meetings and other details. A pragmatic all-encompassing definition, which informs the work in IRISS is given by Steyaert/Lisoir[374]:

ñ*A focus group is a planned discussion among a small group (4-12 persons) of stakeholders facilitated by a skilled moderator. It is designed to obtain information about (various) peopleôs preferences and values pertaining to a defined topic and why these are held by observing the structured discussion of an interactive group in a permissive, non-threatening environment. Thus, a focus group can be seen as a combination between a focused interview and a discussion group.***ò**

---

371 More details of the FG in IRISS can be found in Annex 1 ñTask 4.3. Handbook: IRISS Task 4.3 ñInformed Debate on Surveillance and Control: Methodological basis and organisational Guidelines.ò

372 Merton, R. K. and P. L. Kendall, The Focused Interview. *American Journal of Sociology*, 1946, 51, pp. 541-557.

373 DürrenbergerR, G. and J: Behringer, *Die Fokusgruppe*, Stuttgart, 1999.

374 Steyart, S. and and H. Lisoir (eds.) *Participatory Methods Toolkit ï A practitionerôs manual*, Brussels: King Baudouin Foundation and the Flemish Institute for Science and Technology Assessment (viWTA), 2005.

Summing up: a FG basicallyé

- consists of 4-12 people,
- needs a stimulus for triggering the discussion,
- is a moderated discussion,
- that needs an open climate and
- is non-directive.

Settings in different countries

The FG were held in the participating countries during February and March 2014. A Handbook[375] with organisational guidelines was prepared by the task leader and sent to partners in December 2013. In order to get comparable results more easily a Template of Analysis[376] was provided to the partners in February 2014. According to the Handbook participants in FG I and II were supposed to meet several criteria. First and above all participants in FG II should not previously have been in contact with the project. The ñcontrol groupò was recruited randomly using different communication channels including social media as well as printed materials (flyers). Participants of FG I were recruited from the pool of interview partners from Task 4.2. Furthermore participants of the FG were supposed to meet certain very rough socio-demographic criteria e.g. gender (equal distribution), age (18-30, 31-60 and 60+) and educational level (vocational training, secondary school or equivalent,, academics). It turned out that overall the recruitment of participants was much easier for FG II (the newly recruited ones) than for FG I (those who have been interviewed already by IRISS partners). This is reflected by a higher number of participants on average and a more equal gender balance achieved in FG II. With regard to age the distribution in both kind focus groups was more or less equal. Overall in both groups in all countries academics were overrepresented, whereas participants with vocational education were represented in two countries only.

A full picture of the structure of the FG in the different partner countries can be found in the table below:

	FG I					**Sum**	**%**	**FG II**					**Sum**	**%**
	AT	**G**	**IT**	**SLO**	**UK**			**AT**	**G**	**IT**	**SLO**	**UK**		
Participants	3	4	7	6	5	25		8	6	6	7	8	35	
Female	3	2	5	3	2	15	60%	4	3	3	3	4	17	49%
Male	-	2	2	3	3	10	40%	4	3	3	4	4	18	51%
Age														
18-30	1	-	1	6	-	7	32%	1	-	2	7	1	11	31%
31-60	2	2	6		4	15	56%	5	5	4		7	21	60%
60+	1	2	-		1	4	16%	2	1	-			3	9%
Education														
Vocational		2	2		-	4	16%	-		-			-	0%
Secondary school	1	1	1	1	-	4	16%	3	3	4	3		13	37%
Academic	2	1	4	5	5	17	68%	5	3	2	4	8	22	63%

Table: socio-demographic structure of FG participants

375 See Annex III ñTask 4.3. Handbook: IRISS Task 4.3 ñInformed Debate on Surveillance and Controlò

376 Ibid.

In the beginning of all FG a short introduction to the issue at stake was provided to the participants. This rather short, 5-10 minute, introduction opened up the theme and framed the following discussion. In the IRISS project we decided to take advantage of the international attention surveillance has received through the Edward Snowden revelations. In the handbook a text was provided, which was used by the facilitators according to their national needs. Besides the common definitions and explanations we also provided the participants with some possible reactions to the global surveillance scandal. The project team looked into the IRISS database and presented some quotes from the interviews to illustrate attitudes that emerged during the interview series. Reactions to the Snowden/PRISM scandal ï the ñglobal surveillance disclosureò could in our terms be categorized either as ñraised awarenessò, ñneutralisingò, ñignoringò or ñascribing political relevanceò to the issue. Using some of these quotes, we built a common basis for the following discussion.
All partners succeeded to organise the FG without major problems. Providing incentives like book- or fuel-vouchers up to ú 30 per participant supported the recruitment. In UK vouchers for a local cinema or a bookstore were given after the FG as a token of appreciation. The FG were conducted and moderated by partners themselves or by external moderators.

All partners analysed their respective FG and provided national reports to the task leader. These national reports are building blocks of the findings described later.

Research questions

Task 4.3ôs main objective was to find out whether there are differences in attitudes, values and lines of argumentation between participants who were interviewed in depth and those who hadnôt had contact with the project before. One working hypothesis was that the previously interviewed participants had more time to reflect, that their awareness of the issue at stake had been raised by the in-depth interviews and therefore their way of arguing ï in whatever way ï may be more concrete and reflected.

Conducting the FG in five European countries obviously raises the question of different attitudes in different countries, political cultures, broadly speaking ï environments. It should however, by clearly stated that two focus groups with 4 to 8 people per country are by no means an instrument to gain insight into national or cultural differences. Nevertheless analysing the different discussions gives insight into different surveillance cultures[377] that might have influenced the way discussions went in different countries.

9.4.2 Findings from the national events

In this section we provide an overview of the findings from the FG in the participating countries. This section is based entirely on the national reports provided by the partners. First there is a summary of the respective national events, followed by an in-depth analysis.

Austria

Walter Peissl

Summary

The Austrian FG I and II were quite different. First they were different in size: FG II consisted of eight participants and FG I of only three; FG II had an equal gender balance whereas FG I had only one female participant. The opinions in FG II were quite diverse with a slight tendency of being critical

377 Lyon, David, Situating surveillance ï History, Technology, Culture in Kees Boersma, Rosamunde van Brakel, Chiara Fonio, Pieter Wagenaar (Eds.) 2014, *Histories of State Surveillance in Europe and Beyond*, Routledge, 2014, pp. 32-46.

towards surveillance. Only two out of eight participants were explicitly in favour of surveillance, whereas the others were quite critical and only saw minor positive effects in state surveillance. Participants of FG I unanimously regarded surveillance as negative with only minor or questionable effects on security. Both FG experienced a positive atmosphere and lively discussions. Whereas the FG II spoke rather theoretically about surveillance and its probable effects, in FG I concrete examples, mostly from personal experiences, made the discussion much more concrete. In both groups the attitudes of individual participants did not change after the group discussion. All participants were satisfied with the atmosphere and thankful for having the opportunity to talk about an issue that affects their everyday lives. All expressed their gratitude to the others for having enriched their scope on the issue at stake.

Comparison FG I and FG II

Introductory story, reactions and surveillance in general

In FG II the opinions on the stories and the Snowden revelations were quite diverse. The participants on the one hand stated that there has always been surveillance or questioned the issue as such ï ***ñ****Why do we do that? To increase security, but we actually don****â*** *know what security means* ***ï*** *it means different things to different people.****ò*** On the other hand there were legal-positivistic approaches: ***ò****What is evil is described in the criminal code.****ò*** and also statements that finding proportionality is an almost impossible task. At least two participants remarked that they turned from fatalism (***ñ****you cannot do anything about it****ò***) towards more sensibility and interest in the political dimension of surveillance. The majority was sceptical of and against surveillance or were at least unclear what the real effects could be. Out of the eight participants from FG II only two made a clear statement pro surveillance. One argued from a security point of view and the other from a business perspective. A short discussion on Facebook showed that only few participants were active users, the pro surveillance participants just stated, ***ñ****You have to know what you post****ò*** and ***ñ****The world may know what I post****ò***, demonstrating great confidence of being able to manage data on FB, but probably not fully aware of the mechanisms in the background. The non-Facebook-users were rather sceptical and essentially based their judgement on rumours. All together the discussion was more on a theoretical/vague level, whereas in FG I the participants immediately jumped into the discussion with concrete examples and clear ideas of potential consequences or groups of victims.

The discussion rapidly moved on to the newly introduced electronic patientsôrecord system in Austria and the regulation that stipulates the installation of Smart Meters in 90% of private homes by 2019. This was seen as a precursor to surveillance. Besides this, one participant also mentioned individual concerns, besides the political societal aspect, and her ultimate aim to keep up informational self-determination.

Positive and or negative effects of surveillance

In the discussion on positive and negative effects of surveillance in FG II, some participants neglected positive effects, whilst others saw potential in the increase of security, although this was also questioned. It was not clear how the efficacy of surveillance could be measured. ***ñ****The bad guys always find a way to circumvent the surveillance.****ò*** Essentially, all participants more or less agreed that some surveillance is necessary for the sake of security but they also strongly argued for proportionality: ***ñ****Do only as much surveillance as needed****ò*** (acknowledging that finding proportionality is a difficult task). They also discussed control mechanisms for watching (controlling) the watchers and made a clear distinction between spaces with (accepted) surveillance and spaces that should be left without.

With regard to the negative effects of surveillance, the concern was about long-term consequences, which cannot yet be assessed and for which it might already be too late. From this point the discussion moved directly towards the distinction between public and private surveillance although participants showed more understanding for public surveillance (needed to gain security). Private surveillance with

loyalty cards, credit and debit cards etc. was seen as much more problematic. One participant highlighted the ñvoluntary characterò of these kinds of data collection, although others counteracted this by arguing that it seems hard to resist these subtle methods of seduction. As could be shown the discussion in FG II was diverse with a slight trend of scepticism towards surveillance, although the discussion remained rather theoretic and ñphilosophicalò.

In contrast, in FG I the positive effects of surveillance were more or less neglected by all participants. They saw advantages only for the security industry and other suppliers. Potential positive effects are rapidly turned into negative ones by ñthe greedy nature of human beingsò. There was a rather long discussion on the missing trust in the efficacy of surveillance measures. This was enriched with personal experiences of fingerprint systems at border controls. Furthermore it was discussed that e.g. CCTV may help in criminal prosecution but cannot prevent criminal actions. This was illustrated by a recent case of rape in the Viennese underground. On a more theoretical level the individual loss of control over oneôs own life was seen as a negative effect of a ñpreventiveò or ñsecurityò society.

Discussing private versus public surveillance

In FG II it was agreed that there is a difference in assessing public and private surveillance. The state should be in charge of providing security and for that reason surveillance may be accepted to a certain extent. At the same time it was acknowledged that boundaries are blurred and a strict distinction between public and private ï even if desirable ï is no longer realistic. Private in this context was discussed in different settings. On the one hand, even surveillance by public authorities, which is accepted, should respect ñprivateò activities like email communications and rather focus on ñopen, public placesò (implicitly thinking of CCTV systems). On the other hand, ñprivate activitiesò ï surveillance by firms via loyalty cards, location based data etc. ï was deemed problematic. In this respect the group was divided into three groups: the majority was critical towards private surveillance, two participants were in favour and one participant felt confined by subtle mechanisms of seduction and direct economic pressure. The participants in favour of private surveillance activities referred to its voluntary nature and to legal mechanisms of protection. All together the participants expressed a high degree of trust towards the state, public institutions and the law (Data Protection Law etc.).

Participants in FG I did not differentiate between public and private surveillance and both were rejected. Again concrete examples of disadvantages for consumers were discussed (e.g. ticket pricing using the order-history, which resulted in higher prices for frequent flyers ï erasing cookies or changing computers made tickets cheaper again. Special attention was given to developments in technology-use in the family context and the issue of trust and control. Easy plug and play technologies deliver surveillance potential almost everywhere, which induces unreasonable suspicion. Finally the participants discussed ñfearò as a cultural phenomenon tackled differently in various parts of the world.

Who should participate in decision making on surveillance measures?

Statements in FG II with regard to decision-making circled around capitalism, expert interests, politicians and science. Technology development is capital intensive and therefore economic interests dominate and push developments. The participants agreed that there seems to be no chance of revoking recent developments and they shared scepticism regarding awareness of politicians. One of the suggestions was to ask independent scientists (as in TA institutes) to give an overview of the state of art. Toward the end of the discussion, participants discussed and were broadly in favour of the idea of involving children in the decision-making process, as it is their future at stake.

In FG I the participants argued for the involvement of all persons affected by surveillance technologies, although at the same time some concerns about direct democracy arose. However, participants raised the point that decision making with broad public involvement requires prior

education and information. Critical questions that arose in this context, related to who will do that and how this could be done in an objective way? Participants were in agreement about ethical issues surrounding technical developments and made the claim that ñnot everything thatôs possible, should be doneò. In contrast to FG II, in FG I a statement was made in favour of engaging the in decision-making, due to their considerable experience.

Did this FG change your mind?

With regard to this question, there was no difference between participants of FG I and FG II. They were thankful for having had the opportunity to express themselves, to learn from others and to increase their knowledge on the issue at stake. Almost all participants stated that they did not alter their attitudes in the course of their involvement, but were satisfied by the quality of the discussion. One participant stated that he learned that ñsurveillanceò can have also positive connotations: in the field of (intensive-)care and with regard to caring for children.

Germany

Daniel Fischer

Summary

The discussion in FG I can be summarized as follows:

All participants contributed stories about what they had heard or experienced, to develop a common idea of surveillance. The discussion was very elaborate, as participants differentiated between data production, data analysis and decision-making based on the results of the analysis. De-contextualising data and using them out of context was considered problematic. All four participants agreed that surveillance is far too complex to be managed properly. A mother of a 9-year-old boy expressed the need to protect her son from ubiquitous and permanent efforts to influence his consumption. Another participant tried to draw a more relaxed picture of the situation: ***ñ****In the end itôs me who decides what I buy, and as long as this is the case, thatôs ok.****ò***

The last major topic was about institutional responses: This started with a spontaneous call for more transparency, although the group changed its opinion in the course of the discussion: Based on mistrust of government, ñtransparencyò would hardly be accepted without significant doubts. It was also argued that transparency would probably be impossible to achieve due to the amount of information involved. One participant posed the question whether ñ*knowing everything*ò might not frighten people more, than the current situation of ñ*not knowing about most things*ò.

The discussion ended with some concluding remarks, which can be summarized as follows: Circumstances are not easy to influence and change. This can lead to a) an even more desperate struggle against ***ñ****it all****ò***; b) to extremely time consuming discussions about the topics without having an effect, or c) to a relaxed state of personally not feeling surveilled.

The discussion in FG II can be summarized in four parts:

Participants were not in agreement. The elder participants were more concerned with privacy issues, whilst the younger participants presented themselves in a somewhat controversial manner: A mixture of being careless, resigned, incautious, and inconsistent.

We then asked participants to talk about surveillance in all walks of life, and how they reacted to it. This conversation centred mainly on security related state surveillance. Although there were several different positions on the issues discussed, this did not lead to controversy, but rather to a neutralisation of experiences. Whenever a participant raised a concern, another participant tried to erase the concern by demonstrating the lack of alternatives; e.g. ***ñ****why worry about things you canôt change?****ò***

ñ*GPS tracking might be bad****ò*** -> ***ñ****You can be tracked either way.****ò***

ñEncrypting mails might be a good thingò -> ñIt will get hacked either way/is it that important what you writeò
ñFighting terrorism might be worth all that.ò ï ñThereôll always be terrorism.ò
ñCCTVé well é of course there are pros, of course there are cons, leave me alone with it.ò
A mood of *ñDigging deeper here wonôt bring us furtherò* pervaded the discussion, there was a preference to leave things as they were.
Participants were not really concerned about surveillance by private actors. All considered themselves quite prepared against being seduced to buy things they donôt want. Again, the main thrust of the discussion was the lack of convenient alternatives to WhatsApp, Facebook etcé
The dominant mode converged on a kind of fatalism: *Yes this is problem when you really think about it ï but I cannot think about it all the time.ò*

Comparison FG I and FG II

Differences

The participants of FG I (informed) were ready and willing to identify with the topic and were very interested in the opinions and experiences of the other participants. They tried to synthesise all points raised to create a ñbigger pictureò of the direction in which surveillance society could go. There was an interest in developing a common opinion at least about the current situation.

The participants of FG II appeared to be much less willing to identify with the topic. Although initially, participants uttered one or two standard statements, this did not lead to a committed debate. Everybody brought up their own experiences with surveillance, but nobody tried to create some sort of ñcommon destinyò out of which a demand for action might arise. Although some participants shared similar experiences, this was largely considered to indicate normality rather than being questioned.

The participants of FG I were either looking for ways to avoid surveillance (more civil engagement, fewer cameras, not giving away data if it isnôt urgent, using secure technologies). Arguments to voice protest against surveillance were raised. This process of ñlooking for alternativesò however, proved to be more than frustrating, since new insecurities kept arising. Toward the end of the discussion, participants delegated responsibility ñback to the governmentò, despite a natural distrust of government authorities.

In contrast, participants of FG II were much more sceptical about *real* options. They did not have any utopian ideals about a surveillance-free society. Although they acknowledged that things probably go wrong, in the end they came to the same ñconclusionò as participants in FG I, although discussions were considerably shorter: delegate final responsibility to the government. FG II participants stated that it is beyond their capabilities to act appropriately in relation to surveillance. Overall, participants of FG II remained much more relaxed and focused on their daily routines than participants of FG I and simply accepted the status quo:

- They envisaged surveillance as something normal that has always existed and will change and develop parallel to society,
- and they accepted economic and political interests and the possibility of manipulation based on intelligence/data

In both groups arguments and attitudes did not differ on the basis of gender, although there were generational conflicts in FG II, which did not surface in FG I. In FG II, the two elder participants had more concerns about any surveillance related (online) communication activities than the younger participants, although the elderly were less affected by it (as they spend much less time e.g. in the Internet than others).

Similarities

- All participants were pretty well informed about surveillance in general.
- Participants were particularly knowledgeable about CCTV, which played a central role in the discussions in both groups. Cameras still serve as the classic symbol of surveillance and views toward them are ambivalent (care and control/security vs. freedom).
- In both groups, surveillance was perceived as a collectivizing phenomenon. Participants did not feel monitored individually, but rather that ñsocietyò is under surveillance. FG I participants argued that ñsocietyò should be motivated to resist surveillance in some way, whereas FG II participants, tried not to deal with this topic any more than necessary.

Italy

Chiara Fonio, Alessia Ceresa

Summary

The motivations of various participants from FG I were as follows:
ñ*The individual interview has stimulated my curiosity and I want to look into this issue in more depth, as I didnôt know about this and usually, due to laziness, we avoid looking for more information on something we donôt know anything about and we donôt really think about the importance of this issue.*ò
ñ*Itôs a topic that involves our everyday life, but we really donôt think about it and we donôt have much information on surveillance and CCTV systems (é)*ò
ñ*Iôm already very sensitive about this issue (é) as Iôm annoyed about loyalty cards, since I feel spied on whilst I am shopping or by the electronic register at school, etcé .therefore, I accepted the chance to be interviewed immediately and to attend the FG now (é)*ò

In contrast, participants from FG II indicated curiosity as their primary motivation for attending:
ñ*Iôm interested in the issue*ò, ñ*Iôm curious about this particular experience*ò, ñ*Iôm interested in exchanging and getting information on this issue*ò and ñ*Iôm curious to experience a FG and Iôm interested in technological devices.*ò

The two Focus Groups have demonstrated that the perception of the ñsurveillanceò issue is increasingly becoming a global phenomenon, i.e. it goes beyond national frontiers and it is a trans-generational problem as well, since it involves citizens of all generations within a certain society.

The perception that surveillance has to be analysed from a supra-national perspective is due to different factors. On the one hand, globalization, referred to as an economic and financial phenomenon in this instance, increasingly plays a role, covering ever more aspects of our everyday lives, including surveillance practices. On the other hand, the rapid evolution of new technologies and the implementation of technological devices have led to a general perception that the two terms, i.e. surveillance and technology, are complementary and, in certain cases, even overlap each other.
Participants deemed both surveillance and security to be international phenomena that have to be dealt with by the ***ñ****International Community****ò***.

A further issue, involving both the discussion groups, is the problem of lack of information (considering also information overload and disinformation), since citizens often perceive themselves to be ñvictimsò of ñsurveillanceò even if they are not familiar with the topic of surveillance. This is on the one hand due to a general lack of active involvement in public debates. The lack of information is crucial as well, i.e. information received by citizens from the public sector (institutions, entities,

agencies, etc.), the private sector (companies, corporates, etc.) and mass media (newspapers, TV, radio, as well as the Internet, social networks, blogs, etc.).
It is interesting to note that this aspect is directly related to a more general ñlack of awarenessò which emerged specifically from FG I. In fact, the level of information, both from a qualitative and quantitative perspective, can function as a trigger in order to develop a higher level of awareness among citizens within ñsocietyò.

Comparison FG I and FG II

A comparative analysis of the results of the two Focus Groups, from a question-by-question perspective, reveals that there are substantial differences and commonalities between the discussions.

In general terms, a comparison between the two groups reveals that FG I, attended by people who experienced the individual interview, had a clearer idea of surveillance, demonstrated by bringing in concrete examples from their everyday lives. In contrast, the second group had more problems providing effective stories experienced during their daily lives.
Furthermore, while participants attending FG I were able to talk about surveillance from a pragmatic perspective, suggesting concrete solutions to the problem, the second group, for the most part, was only able to talk about the topic in more theoretical terms, perceived as an issue we are used to reading about in the newspapers and which is difficult to detect in our everyday life.

Similarities

An in-depth analysis of the two groups, in fact, reveals that there were more differences than commonalities between FG I and FG II in terms of opinions and suggestions.
The commonalities can be expressed as follows:

- *What do you think about surveillance in general?*
  Both FG I and FG II perceived the issue of ñsurveillanceò in terms of a trade-off between ñSurveillance vs. Securityò: i.e. we need to renounce some of our freedoms and tolerate some surveillance practices in order to live a safe/secure life
- *Who should be involved when deciding on implementing new surveillance measures?*
  Both groups were more tolerant towards public, as opposed to private surveillance, because of the idea that public entities manage surveillance practices in a more responsible way, since their aim is the protection of citizens (i.e. safety/security.)
- *Has your participation in todayôs event changed your attitude towards surveillance? If so: Why?*
  The participants in both FG, in the end, noted that the experience of the discussion group did not change their original opinions, but it helped in highlighting some aspects on surveillance they would not otherwise have thought about. The FG were an opportunity to collect and exchange ideas, as public discussions on the issue are very rare.

Differences

The following differences emerged from a comparison between the two discussion groups:

- *What are your immediate thoughts about the stories heard?*
  The two quotes (i.e. ñEdward Snowden caseò) used to open the discussion were interpreted in different ways: FG I commented on it from a practical perspective (i.e. concrete examples), while FG II perceived the two opinions from more of an abstract point of view.
- *What do you think about surveillance in general?*
  FG I defined ñsurveillanceò as something concrete that influences everyday life, while FG II couldnôt provide a clear definition of the issue, as they perceived it more from a theoretical perspective.

- *What do you think are important positive or negative potentials of surveillance?* Positive aspects of surveillance for FG I were crime suppression and the facilitator factor in law enforcement. FG II was reluctant to find positive aspects of surveillance. Negative aspects for FG I were identified a priori with the necessity to define a concrete motivation for surveillance practice, while FG II identified the negative aspect of surveillance as the ñ*misuse of personal data*ò.
- *Who should be involved when deciding on implementing new surveillance measures?* Whilst FG I thought that citizen should be addressed through a referendum, FG II preferred to involve citizens through an indirect channel, such as via NGOs or associations.
- *Do you have any suggestions about the regulation of implementation of surveillance measures?*
  FG I suggested implementing regulations, organizing more public debates and developing the ñculture of securityò among citizens and considered the implementation of ñethical codesò from the (public/private) entities perspective a necessity. FG II limited suggestions to the generic implementation of ad hoc laws. Both FG I and FG II underlined the necessity to act on an international level (i.e. ñglobalization effectò).
- *Do you have any final remarks, points or messages that you would like to add?* Although both FG I and FG II underlined the ñlack of informationò about surveillance in our society, FG I noticed that the ñlevel of awarenessò is directly proportional to the information provided.
-

General terms of comparison

In general terms, a comparative analysis between the two Focus Groups reveals that the individuals attending FG I and FG II in Italy can be classified, as far as profile and behaviour goes, within two basic categories: i.e. experts and lay participants:

- Expert: an individual who, on the basis of his/her education/profession/personal interests, is familiar with the surveillance issue in general and/or is familiar with technological devices, intended to be the most diffused means for surveillance practices,
- Lay: an individual who experiences surveillance as an ordinary citizen in his/her everyday life, with a basic technological knowledge or no ICT knowledge at all.

These descriptions show that the positions taken by individuals from the two categories are substantially different, although it is interesting to underline that this aspect is more evident in participants attending the second Focus Group. In fact, the lack of interviews with researches has been crucial in influencing both the behaviour and the results of the people attending the FG.

Experts perceived surveillance practices as something to be taken for granted. Lay participants can be divided into two sub-groups: i.e. individuals who were shocked and scared about the issue, which, although they perceive as always present, they know little about; and individuals who are getting used to and accept surveillance, at the same time, exploiting opportunities that have emerged from this practice, i.e. technological devices.

It is also important to consider age as a factor that influences approaches towards surveillance: In fact, younger and older participants perceived this issue from different points of view. Put concisely, young people are more accustomed to technological devices as they consider them a part of their everyday lives, without considering potential dangers, in spite of the ñsurveillance factorò being strongly related to the technology issue. The older people, on the contrary, use the technological devices with a more critical approach as they are frightened about the potential dangers and they consider increasing

surveillance in our society as a consequence of the rapid evolution of new technologies, largely diffused in the wider market.
In order to define the various attitudes towards the issues under discussion, it is necessary to develop a model in which the behaviour of participants from both FG is classified. It is possible to create the following typologies on the basis of two attitudes representing a dichotomy:

- Interested Active or Pro-Active / Passive: attitude towards surveillance in everyday life. Interested Active are individuals interested in surveillance, who donôt take action for/against surveillance; Pro-Active are individuals interested in surveillance, who take action for/against surveillance; Passive are individuals who are not interested in the surveillance issue at all.
- Resistant / Open to change opinion: attitude towards surveillance after the FG experience.

It is possible to draw a diagram of the ñcategories of individualsò (i.e. Expert / Lay) and the ñtypologies of behaviorsò pertaining to the participants of FG I and FG II (Interested Active or Pro-Active / Passive; Resistant / Open to change opinion), as follows:

FG I: 7 participants out of 8

Individualôs profile: Gender and Age	**Expert / Lay**	**Interested Active or Pro-Active / Passive**	**Resistant / Open to change opinion** (after FG experience)
Female, 52	Lay	Passive	Open to change opinion
Female, 40	Lay	Pro-Active	Open to change opinion
Female, 45	Lay	Pro-Active	Open to change opinion
Male, 42	Expert	Pro-Active	Open to change opinion
Female, 52	Lay	Passive	Resistant
Male, 24	Lay	Interested Active	Open to change opinion
Female,50	Lay	Interested Active	Resistant
Female, 75	(did not attend FG)	-	-

FG II: 6 participants out of 8

Individualôs profile: Gender and Age	**Expert/Lay**	**Interested Active or Pro-Active / Passive**	**Resistant/Open to change opinion** (after FG experience)
Female, 23	Lay	Passive	Resistant
Male, 24	Lay	Passive	Resistant
Male, 53	Expert	Passive	Open to change opinion
Female, 60	Lay	Interested Active	Resistant
Male, 35	Expert	Pro-Active	Open to change opinion
Female, 52	Lay	Passive	Resistant
Female, 49	(did not attend FG)	-	-
Female, 26	(did not attend FG)	-	-

In conclusion, a comparative analysis of both diagrams reveals the main difference between FG I and FG II: namely, the ñrigidò (i.e. ñresistantò) behaviour of the participants in FG II due to a generally ñpassiveò attitude towards surveillance, due to an a priori lack of information on the topic which hampered the development of awareness of, behaviour toward and opinions on the issue. On the other hand, FG I is more ñactiveò, since the a priori experience of the interview, as mentioned by all participants, contributed to an increase in their level of information, as well as their level of knowledge on surveillance, as this stimulated them to collect more information on the issue.

Slovakia

Erik Láġtic, Martin Kovaniļ

Summary

The discussion about the quotes started with an opinion, that we should not be surprised by what the Snowden leaks brought to light and that this was to be expected. In general, surveillance was not seen as something negative, rather as something that can protect us. Respondents agreed that intelligence agencies are not interested in our communications and that they are barely interested in the broader picture (aggregated meta-data). Only one respondent voiced a concern, that something like this could possibly be misused in the future and drew a parallel to communist security services archives.

When talking about surveillance in general, a big discussion about the online environment and social networks developed. In this context respondents spoke about the problem of the use of information found online, for various purposes (e.g. employers screening their potential or current employees). Here respondents highlighted the fact that when working with such information, it should be taken into account that information found represents just a fragment of the individual person and needs to be understood in a certain context (e.g. age, social situation in which the picture was taken).
The positive aspects of surveillance identified, are mostly in connection to the use of CCTV for crime prevention. In terms of private entities, use of loyalty cards and gathering of data about consumer behaviour was also seen as advantageous for consumers, since it helps improve products and services.
When it comes to negative aspects, the only thing mentioned was the problem of sharing data that an individual agrees to disclose to a company, with third parties. This is also something that should be regulated in some way.

Implementation of surveillance measures should not be the subject of too much public deliberation (since it is a complex problem and it would be too complicated). Respondents agreed that standard representative tools are sufficient, if they work properly. What is important is information and education in these areas, especially when it comes to digital literacy and this is something that should be implemented in elementary schools.

The discussion started with reactions towards the quotes concerning the Snowden leaks. Respondents predominantly endorsed the ***ñ****nothing to fear, nothing to hide*ò approach, although the opinion, that these practices are worrying was also voiced. The Snowden leaks themselves were not discussed. It was agreed that individual citizens cannot do much about these practices, although it is important to talk about them and spread knowledge on these issues.

When talking about surveillance itself, respondents mentioned a wide variety of practices, with the most focus placed on online surveillance and CCTV ï something that was discussed quite extensively in the interviews. CCTV surveillance is seen as contradictory, with arguments both for and against presented. Online surveillance was seen as having the most possibilities and as a practice, which can generate the most data.

The positive effects of surveillance can be divided into three broad categories. Protection, either by public authorities (CCTV) or by citizens themselves; commerce and the improvement of services, which can be achieved if producers and vendors have enough data about their customers; and an aspect connected with the work environment ï higher employee productivity can be achieved, if surveillance mechanisms are in place. The latter aspect was contested by one respondent who saw too much surveillance at the workplace as counter-productive and an invasion of privacy.

When it comes to the negative effects, the possible misuse of data was seen as the biggest threat. Another negative is the use of incomplete data about a person (data doubles) as a source of information for companies in the hiring process. Some opposition towards CCTV cameras was voiced as well, based on the personal experiences of one of the respondents.

What is interesting is the fact, that the focus group agreed that state surveillance is less trustworthy than private surveillance, which is underlined by general distrust of the state in Slovakia.

Decisions about the implementation of surveillance mechanisms should be left to representative bodies; the focus group did not really see any bigger role for the public in the decision-making process. However they did call for a bigger role of experts and academics, and more data-based approaches in this process.

When talking about regulation, respondents did not come up with any specific mechanisms; however they suggested more transparency on the functioning of these various mechanisms. Also the option of opting-out of some surveillance practices was mentioned.

All of the respondents agreed, that previous experience with IRISS had an impact on their thinking about these issues and in some cases it even influenced the behaviour of some respondents. In the last round, the possibility of connecting the issues of surveillance with the growing popularity of conspiracy theories was raised.

Comparison FG I and FG II

The two focus groups allowed us to identify differences on the topics discussed, as well as on opinions towards surveillance between informed and uninformed participants. It should be mentioned, that FG I lasted slightly than FG II, which can be attributed to the fact that respondents knew a little more about the issues and thought more about the related problems. Problems were to some extent voiced by FG I respondents as well, who mentioned that their previous involvement in IRISS had helped shaped their opinions about surveillance.

Comparison by issues discussed

Concerning the discussion of *Snowden leaks and quotes from previous interviews*, both groups agreed that this is something that should be expected. Both groups endorsed the ***ñ****nothing to fear, nothing to hide****ò*** approach. The main difference was in fact, that FG I voiced some concerns. Participants found these revelations (and practices) disturbing to some extent, however, they all agreed that there is little one can do to avoid it. FG II was more focused on the benefits of such practices, such as provision of security. They highlighted the fact that most likely nobody is interested in their data and the focus is on meta-data.

When it comes to the topic of *surveillance in general*, both groups discussed a variety of topics and came up with a number of examples. FG I concentrated more on the issues that were discussed in the interviews. FG II touched on a slightly bigger variety of topics, although in a less detailed manner. FG I discussed CCTV surveillance and online surveillance in most detail. CCTV surveillance was seen as

contradictory, with arguments both for and against presented. Online surveillance was seen as having the most possibilities and as a practice, which can generate the most data. FG II focused most on the online environment, social media and workplace surveillance, since these were the topics with which they had been in most contact with themselves.

Both groups were able to identify several *positive effects of surveillance*. FG I identified three groups of positive effects: Protection, either by public authorities (CCTV) or citizens themselves, although CCTV surveillance was seen as ambiguous and the positive view was challenged by one of the respondents; commerce and the improvement of services, which can be achieved if producers and retailers have enough data about their customers; and the work environment ï higher employees productivity can be achieved, if surveillance mechanisms are in place. FG II identified two broad effects ï which overlap with the effects identified by FG I. Crime prevention potential (use of CCTV) and improvement of services by the private sector (such as collecting data from loyalty cards).

FG I discussed *negative effects* in more detail. The most prominent issue was the possible misuse of data. Another negative effect highlighted, was the use of incomplete data about a person (data doubles) as a source of information for companies in the hiring process. As has been previously mentioned, some opposition towards CCTV cameras was voiced as well, based on the personal experiences of one of the respondents. FG II mentioned only the problem of sharing personal data with third parties, without the consent of the individual in question. In general, both groups saw more positive sides of surveillance, than negative.

When discussing the *difference between public and private surveillance*, both groups mentioned issues that can be classified as distrust towards the state and its ability to govern effectively. This was more prominent in FG I, who agreed that in general state surveillance is less trustworthy than private surveillance. On the other hand FG II inclined more towards trust in public (state) surveillance, stating that state surveillance has certain, meaningful goals and is regulated. In contrast, private surveillance is interested in profit and one cannot be sure, what is done with the data collected.

Both groups showed a rather high level of distrust towards direct democracy procedures, such as involving the public in discussions about the implementation of various surveillance measures. FG I claimed that *decisions about the implementation of such mechanisms* should be left to representative bodies; participants did not really see any bigger role of public in the process. However they did call for a bigger role of experts and academics, and a more data-based approach in this process. FG II also stressed the importance of educating citizens about such practices. According to FG II it is important to inform and educate in these areas, especially when it comes to digital literacy.

When talking about regulation, FG I did not come up with any specific mechanisms. They only suggested more transparency in the functioning of these mechanisms. Also the possibility of opting-out of some surveillance practices was mentioned. Similar suggestions ï more transparency in the functioning of surveillance, and the problem of data retention were also mentioned.

United Kingdom

Charles Leleux, Keith Spiller,

Summary

This report has documented some of the discussions held at two focus groups in the UK. The comparisons and differences we have highlighted in the following sections have been intended to give some perspective on a group with previous exposure to our research project and one with no exposure.

The geographical distance of over 300 miles between where the groups took place and were recruited from, may give some insight into their views on surveillance and how they are understood in the UK. FG I was more inclined to acknowledge the benefits of data collection and analysis, whereas FG II had a more critical outlook. This may seem surprising, as FG II had no previous dealings with the research project. A number of factors may have produced this outcome: for example, 1) the questions asked in the previous round of interviews may have promoted personal reflection that resulted in participants being satisfied with surveillance and its influence on their lives; 2) participants in FG I may have political or technological leanings that favour the expansion and benefits of data collection, or 3) the propensity of participants ónewô to discussions of surveillance is to presume a negative or suspicious outlook. Our observations are of course prefaced by the fact that we are discussing a limited number of participants and only two focus groups.

Distinctive in our findings however have been some of the similarities and differences held by the groups. Notable, to us, has been the language used by participants and the topics discussed. Particularly evident in the differences between the groups were sceptical notions of trust in various data collecting systems, especially social media, as well as calls for the increased use of surveillance and concepts such as joining up more data dots. These comments we found interesting, mainly in relation to events such as the Snowden revelations and to some degree the attention paid to campaigners such as Julian Assange and WikiLeaks. While it is certainly true that elements of trust did feature in FG I, what we drew upon in this instance was the driver of conversations - for FG II is was a pressing and important issue that was discussed at length and in detail. The same priorities were not expressed in FG I. Again, it is hard to estimate the reasoning behind this, but it does go some way in documenting differing opinions held by the groups.

Noteworthy behaviour in reviewing the similarities expressed are feelings of safety, where the presence of CCTV, as the example most widely used, is understood in terms of reassurance and protection. There is also an interesting dichotomy here as cameras are viewed positively in public environments, whereas, monitoring behaviours in private settings produces altogether more troublesome sensations and behaviours. Nevertheless, a strong consensus remained that UK streets with cameras created safer environments and participants were more inclined to use streets which had cameras. In drawing attention to these examples our intention has been to give a concise overview of the issues and topics discussed in the UK focus groups and to also draw upon a select number of the similarities and differences expressed by participants. In doing so we reason that the report gives a strong impression of the opinions and behaviours of those in the groups and a ósnapshotô of how surveillance is viewed by citizens in the UK.

Comparison FG I and FG II

In general, FG I was more accepting of surveillance and quicker to point out the benefits of data collection and analysis, particularly to catch the ôbaddiesô. Whereas FG II, were more resistant to surveillance-type issues and while they did not seem to be actively resisting surveillance they certainly had a more critical outlook.

Similarities

Potentials or the ówhat ifô scenarios

There was much discussion about political change or the potential dangers of the information generated through surveillance, and its future use for indeterminate purposes - a deep unease with future implications of surveillance was detected with many references to ôBig Brother.ô

FG I

ôWell, I think one difficult thing is, that you could have, as you referred to it, a change in government to a totalitarian state, which could then use this information against people, thatôs one point. Secondly, there is something inherently sinister about government looking at areas of our private experience or what we do, and perhaps we donôt know thatôs happening. So I suppose I donôt like it, but then I can see the sense of, you know, we donôt want to be blown up by a terrorist cell and we want that to be prevented by any possible means. I mean, I sometimes think of the situation with Chile, and that awful man, Pinochet [unclear] *he got a list of the doctors who had and havenôt striked, was it Allende who was there before, and those who had not protested against Allende, in other words, were sympathetic to Allende, Pinochet got them arrested and treated abominably and all the rest of it. So that was a case of using data that perhaps wouldnôt have been expected to be used in that wayô*

FG II

ôWell I think the issue is ówho is going to get the data on me and what are they going to use it for?ô So itôs OK if I have an alibi from a crime etc. but the problem then is: are there other people besides the police getting access to the data. And secondly, well, what happens if the police want to use it for a particular objective, such as, you were talking about trade unions earlier on, Iôm a trade unionist, is that a legitimate thing to be tracing somebody whoôs a member of a political party or a trade union or whatever. And so, what could it be used for besides legitimate crime prevention or crime detection?

Monetization of data

Both groups raised issues around the ócost of free dataô or the monetization of data. Most examples revolved around pop-up ads or how participants were aware that they were giving their information away, albeit to Google, Amazon or other large organisations. Participants seemed happy or accepting of the need to trade their information for access to services.

FG I

óAt the moment itôs all rosy [providing information that the Government may have access to], *at that point does it become monetised, that data? At what point do we become units of currency that can be exchanged for our data, further data rather. Sorry, you must think Iôm being very paranoid here, but I do think of these things as being potentially destructive.*

FG II

*óIôd like to add to this point. In my view the second statement has been on the same side however more in the corporate side of it. Because, as we have spoken before, whether I am cooking something or watching a TV programme could be useful information in corporate terms. And then again, going to a social networking and email services, it is a matter of reading the terms and conditions because pretty much everything is written there and the reason they are free is because they can use the information. Like Facebook we, by clicking ó*I agree with the terms and conditions*ô, we give the rights to use our interests, our comments, our writings to generate information which could be sold to companies who want to sell services or products.ô*

Feeling Safer

There appears to be a widely held belief that CCTV and other devices provide a ócomfort blanketô of sorts. Although a participant in FG II does voice their concerns as to whether or not there is evidence to support this, nevertheless the underlying tone is certainly one of supporting CCTV in the context of personal safety and crime detection.

FG I

ó I mean having all that information, and it can be used for good as well as bad things couldnôt it? I mean, knowing that a percentage of the population are, you know, thereôs things you can find out that might help with, I can think of illness or disease or patterns in society that might tell us things about the way society is developing, those kinds of things, which could be of use and interest, and CCTV camera makes me feel safer. Iôm glad that they can trace people much better now, if theyôve committed previous crimes or whatever. Although you know, I know thereôs the danger that police can, or police can manipulate that. I also know that for me itôs a good thing, because if, you know, something happens I want to know that they can find the person.ô

FG II

ôWell I think personally, it does make me feel a bit safer on the street. Because I think if something does happen, itôs being monitored in some way. Not just me personally but in general, with crime, I just think there is more likelihood of catching a perpetrator. So I feel thatôs a positive aspect of certain street surveillance.ô

Cautious of Control

Evident in both groups was cautiousness about what is going on regarding surveillance in participantsô lives, as well as ambivalence. While most participants freely accepted they have to live their lives with surveillance, they also have a slight uneasiness with how things operate ï possibly Snowden induced, as his name seems to arise more frequently in FG II.

FG I

ó I do worry about the dark side, but I also can see lots of benefits to it too. I find that people sort of mysteriously talk about how bad it is, what a bad thing it is, but Iôm never really clear about why itôs a bad thing and I can also see that there might be lots of good things. Iôm scared of things like mistaken identity, you know, identity theft and all those kinds of things, but I can also see that thereôs a lot of good to it as well. Weôve always collected data historically, looking at history and your job and everything, you know, it would be fascinating information to be able to look at our generation of people, these people that exist now. So I donô know, Iôm sort of in the middle and trying to move about within it.

So I canôt help feel that yes, there are all these wonderful, I donôt disagree with é there are fantastic benefits, and yet, I canôt help seeing, underneath the stone, how can it be, how can it be manipulated. Perhaps too much Bladerunner as a small kid makes me think of these things, but I canôt embrace it wholeheartedly as a wholly positive thing.ô

FG II

ó It was Big Data. I mean at the moment now, even with this Snowdon etc. youôve got to search for the information. But I think when youôve Big Data and you can actually analyse (it) in real terms and know so much about you and then influence your behaviour. Because the thing is they offer you this ófree cinemaô and all of that but they are actually monitoring your behaviour. And this is what really does worry me; the sheer ability in real time to process information about you and then to try to alter your behaviour and you think of all sorts of different ways it can try to do that.ô

Differences

While each of the topics that follow are not unusual in themselves ï they are topics widely discussed in relation to surveillance in the UK ï what strikes us here is the fact that only one group seems to have discussed the matters we highlight below:

Government and private differences

It appears there is a deep-seated ambivalence in the following quote; it is ok to track my online behaviour, but NHS data (and one can presume bank details and other sensitive information) is sacrosanct. Once again nothing unusual in this statement, but the clear division of data and its worth are notable.

FG I

ôI still think thereôs a difference there between the millions, the billions that Google make, because I think they must have the most data, theyôve certainly got the most data on me, and the most valuable data, about shopping and interests and whatever, where I go, and then the NHS selling off our data. To me thatôs just a massively different situation, whereas one needs to be regulated very seriously, and it would be outrageous if that data was sold off, with Google you know thatôs whatôs going on.ô

Powerlessness

There is a very real resignation here in the participantsô comments. They are powerless to do anything. This sense of resignation we felt was less pressing in FG II. Although as the FG II comment below suggests there is a nuanced appreciation that citizens are relatively powerless and everyone is now seen as óguiltyô.

FG I

óPerhaps didnôt think about it enough, but now, whatever you engage with, your computer or if youôre just surfing, you just see that youôre constantly, somebodyôs kind of using everything, you know, youôve ever done, to try and target you. So yes, Iôm much more aware of it, but Iôm not sure what I can do about it.ô

FG II

ôI just want to say on the surveillance, I thought the law was innocent until proven guilty, and I just find surveillance treats everybody as being guilty. Because if you talk about criminality and criminal acts, thatôs what itôs there doing. So itôs assuming thereôs going to be a criminal act and somebodyôs going to perform it. But in the meantime, everybody else has to be watched before that criminal act can take place. And thatôs what I object to.ô

Altering behaviour

A very interesting point is raised here and one that refers to the idea of being watched and how even in everyday terms if we do some menial task it often becomes harder when we know we are being watched. The second comment refers to the fact that most people do not care what they do online ï is this because they are not aware of being monitored? Nevertheless we think the point is pressing in understanding our attitudes and behaviours in relation to what we do online and in other activities.

FG II

ôI think if youôre being watched you do behave differently. And I think also if youôre in a group you behave much more differently if you think youôre being watched. And that doesnôt need to be a positive the different behaviour, it could be very negative.ô

ôI would respectfully disagree with both of you because just think about behaviour online. We now post-Snowden know, even those of us who werenôt as well informed, and people behave as recklessly as they like online. Nobody is careful about - I mean there is no idea of digital citizenship: itôs still quite a ôWild Westô, people are using the internet not thinking.ô

Needs more dot joining

This point concentrates on the need to join-the-dots and to some degree to increase the inter-connectivity of organisations. Here there is a call for greater exchange of data and ôBig Dataô. The notion of inter-connectivity we found interesting and were surprised that others did not voice this point.

FG I

ôWell, very often when they bring up a case, there was one today, child abuse I think, where both the parents had abuse histories, and somebody should have been able to, they should have been flagged up somewhere. The joining up of data between agencies is very poor, they donôt talk to each other, and thereôs no mechanisms for getting it, and it comes up all over the place, when people say, oh well if only the agencies would talk together and the police didnôt know that there had been a threat made against her or whatever, so that would seem like an easier thing to do, if youôd got this database. It seems like a good idea, but youôve got to have a way of protecting it, and I donôt know, I think thatôs difficult to do once youôve gotéif youôve got sort of multiple databases and try and join them together, I think that is probably quite difficult to do, so I donôt know how you would go about it.ô

Displacement of crime

This point speaks to some of the work of Sewell and Barker [378] and how crime and other activities re-emerge or re-fashion themselves. There is recognition here on behalf of the participant that crime is going to happen and there is little that can be done, to stop it, including provision of CCTV. The person seems to be suggesting we are all being misled in a belief that we are safer because of increased technology/security.

FG II

óI think the thing about displacement is if a lot of crime is opportunistic then there could be displacement elsewhere. But another one is speed cameras. Thereôs a huge case about that. Speed cameras are a form of surveillance that is triggered off by a particular event. Although there is a huge debate as to whether they are effective or not. I think one other thing is whatôs the objective? If the objective is to cut crime. There may be another objective which is simply to reduce peopleôs fear of crime. Because generally a lot of the social surveys show fear of crime is far, far higher than actual crime. I mean you were talking about Neighbourhood Watch and so on. Often what youôre doing is reducing, well, there may be social function as well, but you may be just reducing the fear of crime which could be a positive outcome. So people feel safer even though in fact they're not any safer but it doesnôt really matter because youôre actually reducing their fear of crime. So I think thereôs multiple objectives. Itôs a bit like George Orwell in 1984 where they always had war because you always had a war to keep people in control. So the idea was perpetual war to keep the fear up!ô

Social media impacts

This is a significant story that we felt should be included in this section. Evident are the abuses that can, and do, relate to comments placed on social media websites. For a ôVice Consulô or a government official to call a person/visitor/visa seeker to account for expressing an opinion, which could be viewed as problematic ï the penalties for complaining become plain to see. This seems to be highlighting the negative impacts of life online and the consequences of online actions. This was not covered in any great depth in FG I.

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

FG II

ó I think something thatôs interesting about surveillance is itôs a question of level of agency. So I think whether something is surveillance or not is kind of contingent on how much agency you have in that recording of information. But I had an interesting incident happen which I suppose is to do with Facebook surveillance but itôs also to do with crossing state lines online. So Iôm a British citizen and I need a visa to go back to India. And I complained about the service of the Indian consulate on a Facebook public group page. Because there is now this understanding that if you complain on social media it will have a positive impact. I was called in to talk to the Vice Consul and was chastised for an hour! And was told that social media plays a very different role in the Indian government. And this is very true because the Indian foreign minister was sacked after he made - not even defamatory but kind of anti-government statements on Twitter. So itôs kind of interesting that despite, say in a country like India with stakes in technology and its contribution to technology and its advancement, the kind of idea of social media as being a public space which should not be under surveillance is something that theyôre completely not comfortable with. And obviously there are countries that have deeper problems with social networks. Which brings what you were saying about Snowdon etc, that itôs often to do with the kind of idea of a country that they want to portray. So, you know, America wants to be portrayed as doing good, that might not necessarily be the truth.ô

Trust in Social Media Providers and Technology

FG I was slightly more trusting of social media providers and the technology. The issue of trust arises over the relationship between social media providers and the users i.e. can the users trust the social media provider not to share their digital records with other agencies including the state, or is the state or other agencies going to collect the information in any event. Clearly, the Snowden revelations point to the latter, being the case, so in a sense any information, which now has a digital footprint is capable of being monitored and mediated.

FG I

óYes, and you sort of trust the company that you are giving the data to, to look after. But the problem has come about more recently, because that trust has been broken by the governmental organisations, whoôve been snooping on the data, itôs not been the companies themselves. I think Google do a reasonable job of being responsible with the data.ô

ó I do remember sort of finishing Keithôs interview and then sort of feeling I was quite naïve. I still sort of think that, but I also, I kind of think itôs okay, I really, I feel thereôs some sinister elements that I donôt feel engaged with, and I still think Google provide us with useful tools, and we need to pay them something. I think theyôre probably getting a bit too much money, but yesé ô

FG II

óWhat does worry me is, yes they can check your text messages etc. etc. But in the old days you had to get physically listen to your phone now itôs got software. And what really worries me in the next ten years is if the software develops to such an extent that they can actually check - and will check - in real time. Instead of checking one in a million now they can actually check one in one. That really does worry me. So I think the fundamental, what we mean by ósurveillanceô is changing because of technology.ô

9.4.3 Findings: The overall perspective

Walter Peissl

Below we list themes that emerged during FG in different countries. They illustrate the variety of perspectives on surveillance and control. By highlighting similarities as well as differences between the different FG in the respective countries we test the working hypotheses. Furthermore some of the themes below were expressed during both FG I and FG II in specific countries. We therefore show some country specific overlaps or differences.

Regarding the *general attitude towards surveillance* we found similar patterns in the Austrian, Italian and German FG I groups: they were much more critical towards surveillance than the members in the respective FG II. Members of FG I in Austria, Italy and Slovakia were also *more concrete* in their argumentation, negotiated in more detail, brought examples from personal experience and had a clear understanding of ñsurveillanceò, which was probably based on the higher awareness of the issue, due to the engagement in the in-depth interviews in Task 4.2, whereas the FG II in Italy had a more superficial idea of surveillance. This was similar in the Austrian and German FG II, which both had a more abstract discussion and spoke rather theoretically about surveillance. In Slovakia both groups endorsed the ***ñ****nothing to fear, nothing to hide****ò*** approach, with a tendency to see surveillance in general more positively than negatively. In FG II participants touched on a slightly bigger variety of topics, however in a less detailed manner. In the UK participants in both FG seemed to freely accept being part of the system or certainly living their lives with surveillance. However they also had a slight unease with how things operate. FG I (UK) was more inclined to promote the benefits of data collection and analysis. The members of FG II in general, did not see it as something negative, but rather as something that could protect them.

A theme that framed discussions in all FG in all countries was the *surveillance vs. security trade-off*. These debates included a *claim for proportionality and clear limits to surveillance*.
Like the Austrian FG II, all mostly agreed that for the sake of security some surveillance is necessary. The Italian FG I found surveillance acceptable for crime prevention but with strict limits in the individual sphere (e.g. email communication etc.). Both Austrian FG argued strongly for proportionality (***ñ****do only as much surveillance as needed****ò***), acknowledging that finding the proportional approach is a difficult task.

Together with the security issue the question of *public (state) surveillance* was discussed. In Slovakia FG II, participants found positive aspects of surveillance mostly in connection with the use of CCTV and crime prevention. They were more inclined towards trust in public (state) surveillance. They mentioned that state surveillance has certain goals and meaning and is regulated. In contrast, private surveillance is employed for profit and one cannot be sure, what is done with the data. Interestingly, even a member of the essentially positive UK FG I showed a deep-seated ambivalence, as expressed in the following quote: ***ñ****it is ok to track my online behaviour, but NHS data (and one can presume bank details and other sensitive information) is sacrosanct****ò***. Both UK groups were essentially positive towards surveillance, however monitoring behaviours in private settings produced altogether more negative responses and behaviours, due to the personal nature of the data or images involved. This shows that even in less critical groups there are certain limits that are deemed ñintimateò or ñreally privateò.

(Mis-)Trust in public authorities was a driving force behind discussions in both FG in Austria, Germany, Italy and Slovakia. In Italy both groups were more tolerant towards public, as opposed to private surveillance. This also holds true for FG II in Italy and Austria, where members showed more understanding for public surveillance (need to gain security). Private surveillance with loyalty cards,

credit and debit cards etc. was seen as much more problematic. The more critical participants of FG I in Austria made no *distinction between public and private surveillance*, and refused both. In Germany participants of FG I also stated some mistrust in political institutions and the government, although this attitude seems to be considerably stronger in Slovakia. According to the discussions in FG I in Slovakia state surveillance is less trustworthy than private surveillance. Additionally private entities, use of loyalty cards and gathering of data about consumer behaviour are seen as advantageous for consumers as well (FG II). FG II in Germany also stated that people donôt really care much about surveillance by private actors. Private surveillance is deemed more convenient and less critical. At the same time FG II participants in Austria and Italy and participants in both Slovakian FG acknowledged the *blurring boundaries* between public and private data collection.

These blurring boundaries may be one of the reasons that in three out of five countries (Germany, Slovakia and UK) the participants of the FG expressed their concerns that individuals canôt do much about it. The *potentials of surveillance are too huge to be mastered properly* (FG I, Germany), there was a feeling of powerlessness (FG I, UK) and that there is little one can do to avoid it (both FG, SLO)

Part of all narratives in the FG in the five countries was the *iconic character of CCTV* for surveillance. This was expressed literally in all four FG in Germany and Italy and indirectly by taking up the discussion on the efficacy of CCTV in FG I in Austria, Italy and the UK. Most discussions revolved around the statement that CCTV is insufficient in preventing, but maybe helpful in solving crime (FG I Germany) and therefore positive effects of surveillance derive from CCTV as a facilitating factor in law enforcement (FG I, Italy). The only critical appraisal in this respect came from FG I in Austria. Here participants expressed missing trust in the efficacy of surveillance measures in general and CCTV in particular. In Slovakia (both FG) the crime preventing potential of CCTV was highlighted and in the UK (both FG) cameras are viewed positively when they are situated in public environments. There is also a strong consensus, that UK streets with cameras created safer environments.

This ñ*feeling safe*ò was expressed in both UK FG and in both Slovakian groups. Even in the critical FG II in Germany the female participants stated that in certain circumstances women feel safer under CCTV.

More differences emerged during the assessment of the *influence of economy* on surveillance practices. The more critical FG I in Austria and Germany referred to the greedy culture of companies or the greedy nature of human beings. Additionally in Austria participants saw advantages in surveillance only for the security industry and other suppliers. In FG II the Austrian participants understood that technology developments are capital intensive and therefore economic interests dominate and are pushing developments. With regard to the economically induced private surveillance, FG I in Italy recognized that commercial surveillance cannot be avoided and that there are costs of anonymity. That seemed not to pose a problem in the UK, as participants accepted the monetization of data, and they seemed to accept the need to trade their personal information for access to free services. Indeed, participants of the Slovakian FG I saw positive effects of private surveillance in commerce and the improvement of services.

In Italy, Slovakia and the UK the participants in all FG underlined the *importance of information, knowledge and awareness*. A lack of information on surveillance practices in the respective countries was expressed in all groups. Austrian participants articulated their gratitude to the organisers for providing a setting to talk about these practices that affect citizensô everyday lives, and which enriched their perspectives on the issues at stake.

Age played a fundamental role in the debates in different FG. Different generations deal differently with new media and the accompanying surveillance practices. The elder participants were more concerned with privacy issues than the younger ones (FG II in Germany and both Italian FG). The younger participants presented themselves in a somewhat controversial manner: A mixture of being careless, resigned, incautious, and inconsistent. (FG II, Germany). In Austria FG I promoted the idea of engaging the elderly in decision-making on surveillance measures because of their life experience. In contrast FG II participants in Austria appreciated the idea of involving children in decision-making, because decisions on societal level affect their future lives.

The idea of involving the elderly and children in *decision-making* on surveillance measures, demonstrated openness toward broad public debate and participation from the Austrian participants. In contrast the Slovakian participants expressed a rather high level of distrust towards direct democracy procedures in both FG. They rather called for a bigger role for experts and academics, which had also been expressed in FG II in Austria. The Italian participants preferred the use of indirect channels of participation, via NGOs or associations. However the process should be accompanied by a broad public debate involving experts and laypeople.

9.4.4 Conclusion

The overview in this chapter shows widely discussed themes that emerged from different FG in different countries. In the following conclusions we will outline the findings with regard to the research questions and other results from the text analysis.

The main conclusions to be drawn are:
Differences between participants in FG I and FG II could be found.

- Discussions in FG I in four out of the five countries have been much more concrete.
- Discussions in FG I tended to be more critical towards surveillance.

These findings reinforce the working hypothesis that people who have been engaged in the in-depth interviews on surveillance and control, have a clearer picture. Gaining more awareness, they tended to be more critical towards the issue at stake.

However, specific findings show that these results cannot be generalized.

- In the UK FG I was rather positive towards surveillance while FG II was slightly more critical ï in contrast to the groups in the other countries.
- In the Slovakian FG the overall attitude towards surveillance was much more positive than in the FG in the other countries.

These two findings lead to the second research question: are there different surveillance cultures that influence attitudes towards surveillance? Indeed the participants in the Slovakian FG as well as the UK groups included a higher proportion of academics than the other countries and the Slovakian group was much younger on average than the others. As we found the age criterion to be a differentiating criterion in other groups (Italy and Austria) too, we could assume that these criteria together form a specific culture of surveillance. This is underlined by the importance of *age/generation* in the discussions of different FG, where elder participants tended to be more critical and cautious, whereas younger people are more used to the utilisation of new technologies and tend to be less worried about surveillance and control.

Additionally the UK and Slovakia are ñspecialò in a specific sense: the UK may be seen as the ñpioneerò with regard to surveillance measures. Consequentially, people are probably more accustomed to and, meanwhile more accommodating of surveillance than in other countries. Slovakia

is a CEE country, in post-communist era. This could be one of the reasons for a broad acceptance of neo-liberal capitalist attitudes, rating individual economic advantages very highly. At the same time these attitudes could lead to a ñless criticalò appraisal of new technologies. If so, this may account at least for attitudes toward private surveillance activities and the acceptance of collection of data for the purpose of improving services, offering discounts and so on, which were mentioned quite extensively in the FG. A capitalist, entrepreneurial attitude striving for modernisation may therefore be constitutive for the specific surveillance culture. However, the reasons for a rather positive acceptance of public surveillance - such as CCTV remain unclear and could be the subject of further research.

Trust in public institutions was an issue raised in all countries. Distrust of public authorities A was expressed directly in the German and Slovakian cases. This corresponds with the attitudes towards public vs. private surveillance. The Austrian, Italian and UK groups tended to be more trustful of public authorities, using surveillance measures. The rationale was that public surveillance is for a societal good (security) and proper regulation is in place. This was challenged only in the UK and by the Austrian FG II. These participants asked ***ñ****who watches the watchers?****ò*** Private surveillance was considered rather uncritically in Germany and even advantageous in Slovakia.

The most striking results were the security/surveillance trade-off that emerged in all countries and the iconic character of CCTV for surveillance.

In general these FG illustrate, that dealing with an issue can raise awareness, may induce participants to gather further information and promote (critical) thinking. Results from this task far from being representative for European citizens; however, they showed the strong influence different surveillance cultures may have on attitudes towards surveillance and control. The differences between the groups in the UK and Slovakia on the one hand and those in Austria, Germany and Italy on the other, seemed to be more significant than the differences between FG I and II in the respective countries.