www.gw-unterricht.at – ISSN: 2077-1517 Druckversion – ISSN: 2414-4169 Onlineversion – https://doi.org/10.1553/gw-unterricht154s21

Fachwissenschaft

Helena Atteneder*, Bernhard Collini-Nocker** & Thomas Jekel***

„…ich habe ja nichts zu verbergen!“ Zwischen ubiquitärer Geodatenerfassung als Geschäftsmodell und individuell-kontextuellem Geoprivacymanagement

* helena.atteneder@sbg.ac.at, Fachbereich Kommunikationswissenschaft, Universität Salzburg
** bernhard.collini-nocker@sbg.ac.at, Fachbereich Computerwissenschaften, Universität Salzburg
*** thomas.jekel@sbg.ac.at, Fachbereich Geographie und Geologie, Universität Salzburg

eingereicht am: 29.03.2019, akzeptiert am: 23.05.2019

Dieser Beitrag fußt auf den Ergebnissen einer Studie über Smartphone User/innen, versteckte Prozesse der Datenweitergabe und bereitet diese für einen an Schulen durchzuführenden Workshop auf. Das Bewusstsein der Schüler/innen für die möglichen Konsequenzen ubiquitärer Smartphone-Nutzung (massive Datensammlung und -auswertung bzw. Kommerzialisierung dieser Datensätze als Basis zugrundeliegender Geschäftsmodelle – und damit mögliche Eingriffe in die Privatsphäre) soll damit gestärkt, und die besondere Rolle von Geodaten in diesen Prozessen erarbeitet werden.

Keywords: Geomedienhandeln, Geodatensammlung, Geschäftsmodelle, Privatsphäre, Workshopkonzept

“… I don’t have anything to hide!” Between the collection of geodata as a business model and individual-contextualised geo-privacy-management

This contribution is based on the results of a study on (for the smartphone users) hidden data sharing processes and edits these data to be used in a workshop targeted for schools. The pupils‘ awareness of the possible consequences of ubiquitous smartphone usage (massive data collection and evaluation or commercialisation of these data sets as the basis for underlying business models – and thus possible intrusion into privacy) shall be strengthened and the special role of geodata in these processes shall be developed.

Keywords: Geomedia action theory, geodata collection, business models, privacy, workshop concept

1 Einleitung

Die ubiquitäre Nutzung internetbasierter Services auf dem Smartphone geht einher mit einer massiven Datensammlung und -auswertung vonseiten der Service-Provider. Die Kommerzialisierung dieser Datensätze stellt die Basis zugrundeliegender Geschäftsmodelle dar und reicht von zielgruppenspezifischem Marketing bis zu detaillierter Risikobewertung der Bürger/innen. Mögliche Konsequenzen dieser Prozesse für Datenschutz und Privatsphäre werden sowohl aus rechtlicher Perspektive vor dem Hintergrund der im Mai 2018 in Kraft getretenen Datenschutzgrundverordnung (DSGVO) diskutiert, als auch aus einem technischen Blickwinkel der Datensicherheit, sowie auf inhaltlicher Ebene und damit der Frage welche Inhalte Personen über sich im Internet preisgeben. Während auf inhaltlicher Ebene die Diskussion um jüngere Generationen, deren Umgang mit persönlichen Inhalten als besonders freizügig angesehen wird, vorherrscht, wird häufig der versteckte Teil der Datensammlungs-, -kommerzialisierungs-, und algorithmischen Verarbeitungsprozesse außer Acht gelassen. Mit dem Ziel diese Lücke zu schließen, spezialisiert sich dieser Beitrag auf die von Nutzerinnen und Nutzern meist unbemerkte Weitergabe von Meta- und Verkehrsdaten unter besonderer Berücksichtigung von Geodaten.

Unter dem gesamten Bündel der gesammelten Sensor- und Nutzungsdaten nehmen Geodaten insofern eine Sonderstellung ein, als sie räumlich-relationale und räumlich-zeitliche Informationen (vgl. Wilken 2018) über Individuen enthüllen können, die Rückschlüsse auf intimste Lebensdetails ermöglichen. Der Mehrwert, der durch die Erfassung, Aggregation, Filterung und Reorganisation vernetzter Nutzerdaten entsteht, dient als Grundlage von Geschäftsmodellen und wird durch Erfassung von und Kombination mit Geodaten noch gesteigert. *Standort* hat in verschiedenen Disziplinen und Industriebranchen (Gesundheitswesen, Automobil, Verkehr, Bildung, Banken, Unterhaltung, Tourismus, Regierung usw.) an Bedeutung gewonnen und ist zum Kern vieler Geschäftsprozesse geworden. Wilken (2018) spricht von einer nahtlosen Integration von *Standort* in *Services*, also sowohl *Dienstleistungen* als auch (soziale) *Netzwerke*. Diese allgegenwärtige Geodatenerfassung stellt die dritte Generation von Geodatendiensten und -plattformen dar, für deren reibungslosen Betrieb *Standort* auf allen Ebenen unverlässlich geworden ist. Diese Analyse gilt nicht nur für „native" Dienste wie beispielsweise der Fahrdienstvermittler Uber, sondern auch für etablierte Such- und Social-Media-Unternehmen wie Google und Facebook, die zu „ortsbezogenen Serviceplattformen der dritten Generation" geworden sind (Wilken 2018: 26). Diese Dienste und Plattformen erfassen und verarbeiten "geodata at a scale, speed and level of complexity that is markedly different from earlier incarnations of similar services" (Wilken 2018: 29). Geodatenverarbeitung und -auswertung dient nicht nur zielgruppenspezifischem Marketing, sondern dient der Erstellung weltweiter virtueller Gruppen mit ähnlichen Eigenschaften und damit letztlich der Risikobewertung von Bürger/innen. Zur theoretischen Verortung dieser Phänomene hat sich der Begriff „Geomedien" (Fast et al. 2018a; Gryl & Jekel 2012; McQuire 2016) als Überbegriff über „locative media" und „mediated localities" (Thielmann 2010: 5) etabliert um die neuen gesellschaftlichen Bedingungen zu artikulieren, die durch die allgegenwärtige Geodatenerfassung entstehen. Geomedien verweisen auf die Dichotomien, die den Internet-Technologien als Ganzes innewohnen: Sie sind Medien der Ermächtigung, Demokratisierung und des Engagements auf der einen Seite und Medien der Bewertung, Überwachung und Kontrolle auf der anderen Seite. Die nahtlose Integration dieser Technologien in alltägliche Handlungsmuster geht über eine bewusste „Mediennutzung" hinaus und bedarf einer kritischen Auseinandersetzung mit den Auswirkungen – sowohl auf individueller als auch gesamtgesellschaftlicher Ebene. In unserem derzeitigen (westlichen) Gesellschaftssystem, das weniger von *staatlicher* Überwachung und Kontrolle, als vielmehr von einer profitorientierten Verwertungslogik des „advanced capitalism" (Murdock 2017: 123), „Plattformkapitalismus" (Lovink 2016) bzw. „surveillance capitalism" (Zuboff 2015) geprägt ist, muss Geomedienhandeln unter Berücksichtigung ökonomischer Erzählungen analysiert werden. Neben Maßnahmen zur Förderung von Mechanismen zum Schutz der Privatsphäre, die laut Debatin (2011) auf den Säulen der gesetzlichen Regulierung, ethischen Selbstregulierung und privatsphärefördernden Technik (privacy-by-design) beruhen sollten, bedarf es an Sensibilisierungs- und Bildungsarbeit an Universitäten, Schulen sowie Unternehmen.

In einem ersten Schritt beleuchtet dieser Beitrag (Geo-)Datenschutzmanagement auf individueller Ebene in den jeweils spezifischen Kontexten unter Berücksichtigung des „contextual approach" nach Nissenbaum (2010), sowie das Bewusstsein über „versteckten" Datenverkehr in Form von Meta- und Verkehrsdaten und die dahinterliegende Geschäftslogik.

Im zweiten Schritt sollen die Ergebnisse für Bildungsbemühungen im Bereich „Medienbildung" gemäß des Unterrichtsprinzips Medienerziehung (Bundesministerium für Bildung und Frauen, 2014) aufgearbeitet und bereitgestellt werden.

2 Leben in Geomedien

Die Rolle der Medien in der Strukturierung des Gefüges von Gesellschaft, Individuum und öffentlichen Diskursen wird durch eine nahtlose Integration von digitalen, mobilen, internetfähigen Endgeräten in Prozesse des Alltagshandelns auf eine neues Level gehoben. Kombiniert mit Phänomenen der Datafizierung, automatisierten Datenverarbeitung bzw. künstlichen Intelligenz ist es möglich geworden, Entscheidungen zu determinieren, präzise Vorhersagen zu treffen und damit Handlungsspielräume zu beeinflussen. Klassische kausallineare Modelle der Massenkommunikation gelten für diese Phänomene nicht mehr und medien- und kommunikationswissenschaftliche Theorien, die zwischen Produzent/in/Konsument/in, Kanal/Inhalt, zwischenmenschliche/vermittelte Kommunikation, Realwelt/Cyberspace, Privatheit/Öffentlichkeit unterschieden, greifen zu kurz, da diese binären Gegensätze verschwimmen. Wir leben nicht mehr mit, sondern *in* den Medien. „Media are to us as water is to fish" (Deuze 2012: x). Das bedeutet nicht, dass unser Leben von den Medien bestimmt wird, deutet aber darauf hin, dass jeder Aspekt unseres Lebens *in* den Medien stattfindet. Deuze (2012) definiert Medien als „Informations- und Kommunikationstechnologien", als „Maschinen", als symbolische oder technologische Systeme, die die Kommunikation zwischen Menschen

ermöglichen, strukturieren oder verstärken (vgl. Deuze 2012: xii). Der Wandel vom Leben *mit den* Medien zum Leben *in den* Medien hat weitreichende Folgen: Medien sind zu einem notwendigen und unvermeidlichen Teil unseres Lebens geworden. Sie sind allgegenwärtig, können nicht abgeschaltet werden, sind unbestimmt (entwickeln sich ständig weiter) und dienen als Kommunikationsplattformen zur Konstituierung und Reproduktion der Welt, in der wir leben (vgl. Deuze 2012: xi).

Ein Aspekt, der diese mediale Verdichtung ermöglicht hat, ist die Georeferenzierung von Personen, Dingen, Ereignissen, etc. Verschiedene Arten von Geodaten, wie beispielsweise die absolute Lage, relative Lage oder strukturierte bzw. unstrukturierte Geodaten, können unterschiedlich erfasst werden (vgl. Abernathy 2017). Bei internetfähigen mobilen Endgeräten erfolgt die Georeferenzierung meist über A-GPS (assisted GPS), also einen GPS-Sensor, der durch WiFi-Positionierung und die Triangulation von Mobilfunkzellen unterstützt wird, oder über Daten, die als Teil der Exif-Metadaten (Exchangeable image file format) in Bildern geteilt werden. Die Weitergabe durch die User an Dritte erfolgt aktiv, z. B. über WhatsApp, durch den Zugriff auf bestimmte Apps, oder im Hintergrund. Durch Freigabe des Standorts kann die Standort-API von Google kontinuierlich Informationen im Hintergrund extrahieren, um standortbezogene Inhalte zu pushen – bekannt als „Geofencing“ (Barreneche & Wilken 2015).

Das Aufkommen von internetfähigen mobilen Endgeräten mit Zeit- *und* Ortsgenauigkeit ist nicht nur die Voraussetzung für eine Vielzahl neuer Services, sondern auch für eine ganze Reihe neuer Interaktionsmöglichkeiten: Kartieren, Verbinden, Navigieren, nach Personen oder Dingen in der Nähe suchen, „Einchecken“, Beobachten und Kommunizieren (vgl. Abernathy 2017: 24). Unter Berücksichtigung dieser neuen Bedingungen führten mehrere Wissenschaftler/innen den Begriff „Geomedien“ ein (Fast et al. 2018a; Gryl & Jekel 2012; McQuire 2016), der den technologischen (Ricker, 2017) und sozialen Wandel berücksichtigt und sich kritisch mit dieser permanenten *räumlichen* Konnektivität auseinandersetzt. „Permanente Konnektivität“ wird von Steinmaurer (2016) verwendet, um eine neue Art der Kommunikation (ein neues Dispositiv) zu beschreiben, die durch einen neuen Status der individuellen Integration in die technologischen Infrastrukturen digitaler Netze definiert wird. Geomedien rekurrieren auf diese Beobachtung und unterstreichen räumliche Aspekte. Einer breiten Definition folgend umfassen Geomedien alle Repräsentationen von Raum (analog oder digital) und decken ein breites Spektrum an Formen ab: von verbalen Beschreibungen bis zur Visualisierung. „Both theoretical and empirical work suggests that media in general and geomedia in particular set the stage for the appropriation of space by contextualizing communication“ (Gryl & Jekel 2012: 22). Lapenta (2011) argumentiert, dass Geomedien die medial vermittelte Kommunikation und damit das Sozialverhalten regulieren. Sie können als neue Instrumente verstanden werden, die Produktion und Austausch immaterieller Güter, Bilder und Informationen und dadurch die Konstitution immaterieller Räume organisieren (vgl. Lapenta 2011: 2). Unter Berücksichtigung städtischer Bedingungen und des sozialen Wandels nennt McQuire (2016) vier verwandte Trajektorien als konstituierend für Geomedien: „convergence, ubiquity, location-awareness and real-time feedback” (McQuire 2016: 2). „Ubiquity“ bezieht sich auf die Allgegenwart mobiler, eingebetteter und vernetzter Mediengeräte, die überall, jederzeit und auch unterwegs verfügbar sind und durch „convergence“, also durch Verschmelzung von Technologien, Genres und Institutionen geprägt sind. „Location-Awareness“ bedeutet, dass Services an Standort und Mobilität des Nutzers angepasst werden, während sich „realtime-feedback“ auf die Informationsflüsse bezieht, die Echtzeit simulieren, indem die Zeit zwischen einem Ereignis und seiner Medienpräsenz fast auf Null reduziert wird, und Erfahrungen sozialer Gleichzeitigkeit ermöglicht werden (vgl. McQuire 2016: 4). Die möglichen Implikationen von Geomedien reichen von potenziellem Empowerment, Aktivismus und bürgerschaftlichem Engagement (Gryl & Jekel 2012; Gryl et al. 2010; Haklay 2017) bis zu Einschnitten in die Privatsphäre und Überwachung. (Klauser & Widmer 2017; Leszczynski 2017; Murakami Wood 2017)

3 Geodatensammlung, -verwertung und -vermarktung: eine vielversprechende Geschäftslogik

Geolokalisierung ist nicht nur integraler Bestandteil der alltäglichen Smartphone-Erfahrung und der sich ändernden Wahrnehmungen und Aneignungen des Raumes geworden (vgl. Thielmann et al. 2012), sondern auch ein notwendiger Bestandteil zugrundeliegender technologischer Entwicklungen, die häufig von bestimmten Unternehmensstrategien geprägt sind. Soziotechnische Transformationsprozesse werden beeinflusst und geprägt von den jeweiligen Geschäftsmodellen, Profitmaximierungsstrategien, den plattformspezifischen Datenextraktionsverfahren und von algorithmischer, also automatisierter, Datenauswertung der Unternehmen (vgl. Wilken 2018: 21). Insbesondere für Bildungskonzepte zu Geomedienhandeln und Geodatenschutzmanagement bedarf es der Berücksichtigung dieser ökonomischen Pers-

pektive. Geomedien strukturieren Kommunikation räumlich, aber oft auf eine für User/innen unvorhergesehene, teilweise unsichtbare Weise, die einer kommerziellen Logik folgt. Das steigende Interesse an geokodierten Daten und deren Nutzung für einen Mainstream-Markt spiegelt sich im Wachstum der Geospatial Industry wider, die laut Prognosen bis zum Jahr 2020 um 13,6 % zunehmen soll (Geospatial Media and Communications 2018: 4). Der Geoinformationsmarkt hat eine Wandlung vollzogen: „von einem angebots- und großkundendominierten Markt zu einem nachfrageorientierten Massenmarkt, der auch Nischeninteressen bedienen kann" (Fischer 2010: 42). Möglich wurde dieser Wandel durch die Verknüpfung von Geoinformation mit der Netzwerklogik folgenden sogenannten sozialen Medien, die eine Einführung neuer Akteurinnen und Akteure und neuer Produktions- und Absatzpraktiken zur Folge hatte (vgl. Fischer 2010). Der Wandel der klassischen Konsument/innen- bzw. Produzent/innenrollen hin zu sogenannten „Prosumern" (Wortneuschöpfung aus den Begriffen „Producer" und „Consumer") ermöglicht sowohl die Erstellung als auch Nutzung und Filterung nach spezifischen Interessensgruppen, verknüpft mit der Möglichkeit, auch Nischenprodukte anbieten zu können. Für Unternehmen bedeutet das eine teilweise Auslagerung der Produktionspraktiken bei gleichzeitiger Nutzung der so generierten (geokodierten) Daten zur Schaffung neuer Dienste um die Datensammlung und Services zu optimieren. Im nächsten Schritt lassen sich die Datensätze dieser generierten Gruppen weiter vermarkten. Nicht nur der weltweit führende Softwarehersteller für GIS, Esri,(Esri, 2012) profitiert von „location intelligence" (Pitney Bowes Inc. 2007) als Businessstrategie, auch die Kernbereiche der populären Internetnutzung, dominiert von den „Big Five": Google für Suchanfragen, Facebook bei Social Media, Amazon im Online-Handel, Apple und Microsoft im Personal Computing (vgl. Murdock 2017: 123), werden durch die allgegenwärtige Geodatenerfassung neu gestaltet. Sie stehen im Zentrum einer „economy of advanced capitalism" (Murdock 2017: 123), in der das Sammeln von und der Handel mit personenbezogenen Daten ihrer Nutzerinnen und Nutzern den Kern der Geschäftsmodelle darstellt.

Auf individueller Ebene entstehen „new performances of self and re-inscriptions of the body in place and space" (Schwartz & Halegoua 2014: 1656), ein sogenanntes „spatial self" (ibid.); ebenso neue Formen des Identitätsmanagements (Saker 2016), der Selbstüberwachung (quantified self), des Wettbewerbs mit anderen und des „gegenseitigen Beobachtens" (genannt „lateral surveillance" (Andrejevic 2005)). Individuen betrachten ihre eigenen Inhalte durch die Augen anderer – „social surveillance" (Marwick 2012), oder kontrollieren sich gegenseitig: „interveillance" (Jansson 2015).

Wir gehen davon aus, dass große Plattformen von diesen Entwicklungen in dreifacher Hinsicht profitieren: (1) Informationen über individuelle Präferenzen, Standorte und Verhaltensweisen werden gesammelt und (2) mit den einzelnen Netzwerken und Beziehungsgeflechten verbunden. (3) Können die gesammelten Daten zu weltweiten virtuellen Gruppen gebündelt werden; d. h. Gruppen von Personen mit ähnlichen Profilen. Subjekte und ihr soziales und räumliches Verhalten werden kontrollier- und vorhersehbar. Geomedien können daher als „Fortschritt" in einem engen Netz der Überwachung durch Plattformen angesehen werden. Bei der Überwachung durch Unternehmen spielt jedoch nicht mehr „nur" zielgruppenspezifisches Marketing eine Rolle. Die Bildung immer präziserer virtueller Gruppen kann zur Risikobewertung der Bürger/innen genutzt werden (Christl & Spiekermann 2016: 120). Diese Auswertungen können etwa an Finanzinstitute verkauft werden, um Entscheidungen über die Kreditvergabe zu unterstützen (O'Neil 2016); an Krankenkassen, um Versicherungsprämien zu ermitteln; an Arbeitgeber, um Entscheidungen über die Beschäftigung, wie Gehalt und Arbeitszeiten zu treffen oder um die Rückfallquote von Verurteilten vorherzusagen. Vor allem aber können politische Entscheidungen und das Wissen um politische Einstellungen, die sich leicht aufdecken lassen, je nach Staatsform missbraucht werden. Geomedien werfen daher Fragen nach Inklusion und Ausgrenzung, Empowerment und Ausbeutung, Gerechtigkeit und Ungerechtigkeit, Gleichheit und Ungleichheit auf, denn die „'empowering' potentials of mobile connectivity might be hampered by existent power structures that determine what technology is being used, when, where, how and by whom" (Fast et al. 2018b: 2).

4 Geoprivacy

Konzepte der Privatsphäre, die sich klar zwischen dem Privaten (im Zusammenhang mit Familie, Privathaushalten, Intimität) und dem Öffentlichen (kommunikative Netzwerke zur Förderung der öffentlichen Meinungsbildung) unterscheiden, wie sie in der altgriechischen Literatur (Aristoteles) und später in Arendts' (1958) oder Habermas' (1962) Werken zu finden sind, müssen überarbeitet werden, da diese beiden Bereiche durch Prozesse der fortgeschrittenen Geodigitalisierung verwischt und verzerrt werden. Der umfassende Einsatz von Geomedien stellt diese Zwei-Sphären-Konzepte in Frage. Individuelle räumliche Informationen (insbesondere im Zusammenhang mit einem Zeitstempel) sind besonders sensibel in Bezug

auf die mögliche Offenlegung von personenbezogenen Daten (PII – Personal Identifying Information). Kurz erklärt, sind Geolokalisierungsdaten „(1) verteilt, d. h. sie treten auf mehreren Geräten, Anwendungen und Diensten auf, (2) plattformunabhängig – der Datenfluss geht über Plattformen, Dienste und Geräte hinweg und (3) willkürlich, also können potenziell alle Personen davon betroffen sein (Leszczynski 2017: 237). In diesem Zusammenhang wird die Notwendigkeit eines neuen Verständnisses von Privatsphäre durch die „commercialisation of all things 'geo' [represented and fostered by the] ubiquity and ordinariness of locationally enabled devices, mapping platforms, spatial interfaces, geosocial applications and myriad location-based services in the spaces and practices of the everyday" (Leszczynski 2017: 235) ersichtlich. Dieses neue Verständnis von Privatsphäre kann sich nicht mehr an oben genannten Zwei-Sphären-Konzepten orientieren, sollte aber dennoch an bestimmten Werten, Normen und damit demokratiefördernden Aspekten festhalten. Datenschutz und Schutz der Privatsphäre ermöglichen eine freie Entwicklung des Selbst, Selbstbestimmung, Nonkonformität, Vielfalt der Ansichten, Ideen und Möglichkeiten, freie Wahl bei gleichzeitiger Verantwortung und Intimität ohne unerwünschte Einblicke (vgl. McStay 2017: 15, 20). Dies folgt weitgehend Kants Verständnis dieser Bedingungen, wobei Freiheit die Grundlage des sozialen und moralischen Lebens darstellt (Kant 1996). Fried (1970) charakterisiert die Privatsphäre als notwendige Voraussetzung für Liebe, Freundschaft und Vertrauen, die „einem die Freiheit gibt, die eigenen Beziehungen zu anderen zu definieren und sich selbst zu definieren". „Auf diese Weise ist die Privatsphäre auch eng mit Respekt und Selbstachtung verbunden" (DeCew 2018). Im Bereich der digitalen Netzwerktechnologien treffen wir auch Datenschutzentscheidungen im Namen anderer (z. B. Weitergabe von Bildern und Informationen über andere oder Kennzeichnung einer Person). Daher hat Privatsphäre einen kollektiven Charakter, der auf der Interaktion mit anderen basiert (McStay 2017: 21). Wie Nissenbaum (2010) betont, ist Privatsphäre mehr als die Kontrolle darüber, wie viel über uns selbst wir anderen offenbaren, wie bei Westin (1984) beschrieben. Darüber hinaus sind die Strategien für Datenschutz und Identitätsmanagement von kontextabhängigen Aspekten geprägt. Das von Nissenbaum (2010) vorgeschlagene normative Konzept der kontextuellen Integrität betrachtet verschiedene Informationsprozesse in verschiedenen Kontexten. In einem beruflichen Kontext wird eine Verletzung der Privatsphäre anders wahrgenommen als in freundschaftlichen Beziehungen. Aus der Sicht des/der Einzelnen ist das Recht auf Privatsphäre weder ein Recht auf Geheimhaltung noch ein Recht auf Kontrolle, sondern ein Recht auf einen angemessenen Fluss personenbezogener Daten (vgl. Nissenbaum 2010: 127). Was als angemessen angesehen wird, ist eine normative Unterscheidung, die die Schnittmenge von drei Aspekten umfasst: Akteure / Akteurinnen, Sphäre / Raum und Information. Wenn gegen diese Normen verstoßen wird, erleben wir eine Verletzung der Privatsphäre, hier als „Verletzung der kontextuellen Integrität" bezeichnet (Nissenbaum 2010: 127). Auf der politischen Ebene erfordert dies, dass beispielsweise von Regierungen die Bürger/innen mit Respekt und Würde behandelt werden. Angesichts der Macht der Unternehmen in einer kapitalistischen Wirtschaft muss Privatsphäre so konzeptualisiert werden, dass sie Verbraucher/innen und Arbeitnehmer/innen vor unternehmerischer Kontrolle schützt und gleichzeitig Unternehmensinteressen und Unternehmensmacht transparent macht (vgl. Fuchs 2011: 232). Westliches Recht bezogen auf den Schutz der Privatsphäre geht jedoch mitunter mit einem unterschiedlichen Verständnis von Menschenrechten und Ethik einher. Nach Zwick & Dholakia (2001) gibt es zwei grobe Richtungen:

1) Privatsphäre als menschliches Grundbedürfnis und als Bürger- und Menschenrecht (Debatin 2011), vs. Privatsphäre als Ware oder Privateigentum (aus einem kritischen Blickwinkel diskutiert von (Fuchs 2011);
2) Datenschutzbestimmungen und Regulierung durch die Regierung vs. Selbstregulierung.

Verschiedene Länder entwickelten unterschiedliche Strategien. Während die EU-Gesetzgebung Datenschutz als grundlegendes Menschenrecht definiert und eine strengere gesetzliche Regelung eingeführt hat, ist der Datenschutz fast überall in den USA gleichbedeutend mit Privateigentum und wird als Ware angesehen (Zwick & Dholakia 2001: 120). Unternehmen mit transnationaler Reichweite stellen diese beiden Konzepte in Frage, und die Wirksamkeit des jüngsten Versuchs der EU, die rechtliche Regulierung durch die DSGVO zu stärken, muss noch nachgewiesen werden.

5 Self-disclosure und Geodatenmanagement

Auf individueller Ebene sind Strategien zur Verwaltung von Privatsphäre und Identität nach Zwick & Dholakia (2004) von der Genauigkeit und Menge der offenbarten personenbezogenen Daten abhängig.

Dieses Modell (Abb. 1) erweckt den Eindruck, dass die Menge und Genauigkeit der personenbezogenen Daten für die Benutzer/innen selbst, kontrollierbar sind. Es berücksichtigt nicht die verborgenen Schichten des Datenaustauschs.

		Richtigkeit der offengelegten persönlichen Information	
		High	Low
Menge der offengelegten persönlichen Information	High	Identifizierbarkeit	Anonymität / Pseudonymität
	Low	Vertraulichkeit / Diskretion	Geheimhaltung / Verschwiegenheit

Abb. 1: Vier Taktiken des Datenschutzes und des Identitätsmanagements (eigene Abbildung nach Zwick & Dholakia (2004))

In Bezug auf Social-Networking-Sites identifiziert Debatin (2011) mehrere Datenschutzrisiken, denen die Nutzer/innen beim Posten auf Websites zustimmen, und stellt sie in zwei Dimensionen dar: eine horizontale Achse für die soziale Interaktion zwischen den Nutzern und Nutzerinnen (einschließlich Cyberstalking, Belästigung, Reputationsschädigung, aber auch Repräsentation durch Profile), die metaphorisch als *sichtbare* Spitze des Eisbergs dargestellt wird, und eine vertikale Achse für die gesammelten Daten (systematische Erhebung, Aggregation und Nutzung von Daten durch das Netzwerkunternehmen, Data Miner und Regierungsbehörden), die durch den viel größeren, untergetauchten, *unsichtbaren* Teil des Eisbergs dargestellt wird (Debatin 2011: 4 f.).

Abb. 2: „Eisbergmodell“ (eigene Darstellung nach Debatin et al. (2009: 88))

Dieser sogenannte „unsichtbare“ Teil des „Daten-eisbergs“ setzt sich aus Meta- und Verkehrs- bzw. Nutzungsdaten zusammen, wohingegen der sichtbare Teil häufig aus Inhaltsdaten besteht.

- Inhaltsdaten unterliegen dem Fernmelde- und Telekommunikationsgeheimnis und dürfen nur in Ausnahmefällen gespeichert werden.
- Verkehrsdaten sind technische Informationen, die bei der Internetnutzung anfallen und vom Provider verarbeitet und gespeichert werden. Darunter fallen etwa personenbezogene Berechtigungskennungen, Standortdaten, Informationen über die Verbindung und übermittelte Datenmenge.
- Metadaten sind Daten, die andere Daten beschreiben. Sie erleichtern das Suchen, Finden und Verarbeiten bestimmter Datenelemente und sind bspw. gespeichert als Exif-Daten bei Bildern, sehr aussagekräftig (Zeit- und Ortsstempel).

Während ein Großteil der User/innen unter Datenschutz den Schutz der Inhalte verstehen, ist das Bewusstsein für die weit größere Wertigkeit und Aussagekraft von Meta-, Verkehrs- und Nutzungsdaten für die Erstellung von virtuellen Gruppen und eine Risikobewertung durch Unternehmen sowie deren Vermarktbarkeit häufig bei den Usern und Userinnen nicht gegeben (vgl. Atteneder & Collini-Nocker 2018). Auch anderen Autorinnen und Autoren kommen zu dem Ergebnis, dass viele Nutzer/innen häufig nicht über die massiven Datenaustauschprozesse und die allgegenwärtige Überwachung durch online-Plattformen Bescheid wissen (vgl. Christensen 2014; Christensen & Jansson 2015). Es stellt sich die Frage, inwieweit das Wissen über diese Phänomene die Datenschutzstrategien beeinflussen würden. Studien über die Rolle des Wissens über Datenaustauschprozesse, Datenschutzbedenken und Selbstdarstellung (boyd 2014; Marwick & boyd 2014) zeigen, dass Jugendliche in öffentlichen vernetzten Räumen nicht leichtsinnig handeln, aber trotz Datenschutzstrategien die Informationsflüsse nicht ausreichend kontrollieren können, ein Ergebnis, das zeigt, dass ihre technischen Fähigkeiten zum Schutz der Privatsphäre unzureichend sind. Eine von Acquisti & Gross (2006: 21) durchgeführte Studie auf Facebook und anderen Social-Networking-Sites dokumentierte signifikante Dichotomien zwischen spezifischen Datenschutzbelangen und -bedenken und dem tatsächlichen Kommunikationsverhalten bei Schüler/innen und lieferte Belege für das „Datenschutzparadoxon“ („privacy paradox“) (Barnes 2006). Mehrere andere Studien haben die Existenz dieses Paradoxons bewiesen, indem sie eine Lücke zwischen Bedenken zum eigenen Datenschutz und Maßnahmen zum Schutz der Privatsphäre aufzeigten (für einen Überblick siehe Dienlin und Trepte (2014: 294)), und einige Studien zeigen, dass diese Paradoxien, bis zu einem gewissen Grad, erklärt werden können (Debatin et al. 2009). Eine vertiefte sozialpsychologische Analyse der Datenschutzhaltung und des Datenschutzverhaltens durch Dienlin und Trepte (2014) bietet ein komplexeres Bild. Sie unterscheiden zwischen Datenschutzbedenken und Daten-

schutzverhalten und unterscheiden verschiedene Dimensionen der Privatsphäre (informationelle, soziale und psychologische), was zeigt: „privacy behaviors are not paradoxical in nature but […] based on distinct privacy attitudes“ (Dienlin & Trepte 2014: 295).

Was die oben genannten Studien vermissen lassen ist die Untersuchung der spezifischen Rolle von Geodaten. Die umfassende Echtzeit- Geoüberwachung kombiniert mit einer vernetzten Daten- und Geräteökonomie (Leszczynski 2017: 242) stellt besondere Anforderungen an den Schutz der Privatsphäre. Die alltäglichen geomedialen Praktiken sind, so die These dieses Beitrags, geprägt vom Wissen über Datenaustauschprozesse, von kontextuellen Faktoren (u. a. ökonomischen und soziotechnischen Transformationsprozessen), sowie von dem soziodemographischen Status der Nutzerinnen und Nutzer. Im Folgenden sollen die Ergebnisse einer Pilot-Studie in diesem komplexen Bereich vorgestellt und anschließend als Vorschlag für die Unterrichtsplanung im Bereich der Kommunikations- bzw. Medienbildung aufbereitet werden.

6 Geomedien und Datenschutz im Kontext – ein „privacy paradox?“

6.1 Aufbau der Pilotstudie

Die hier vorgestellte Pilotstudie wurde im Rahmen der österreichischen „Langen Nacht der Forschung“ an der Universität Salzburg am 13. April 2018 durchgeführt. Mit einer Kombination aus einem quantitativen Online-Fragebogen und einem Quasi-Experiment [1] wurde das Wissen der Menschen darüber, wie ihre Geodaten bewusst oder unbewusst geteilt werden, erfasst sowie Information zu ihrem alltäglichen Geomedienhandeln und ihren Datenschutzkonzepten gesammelt.

Besucher/innen der „Langen Nacht der Forschung“, in der Regel Familien, Gruppen von Freundinnen und Freunden und Studierende, wurden in Gruppen von 2–6 Personen eingeteilt und durch den gesamten quasi-experimentellen Prozess geleitet. Um maximale Anonymität zu erreichen, lag besonderes Augenmerk auf Datensicherheit und dem Schutz personenbezogener Daten.

- Im ersten Schritt wurden die Teilnehmer/innen gebeten, ihre Smartphones mit einer zufällig generierten SSID (Service Set IDentifier im WLAN) zu verbinden und erhielten ein zwölfstelliges Passwort und eine zufällig generierte Besucher-ID.
- Sobald alle Smartphones einer Gruppe mit unserem WiFi-Gerät zur Erfassung von Forschungsdaten (Meta- und Verkehrsdaten) verbunden waren, mussten die Teilnehmer/innen ein Selfie aufnehmen und mit dem (von uns betriebenen) Webservice teilen (d. h. hochzuladen). Mit diesem Schritt konnten wir die Fülle der als Exif-Daten (Exchangeable Image File Format) enthaltenen Metainformationen aufdecken, wie zum Beispiel GNSS-Koordinaten, Typ des mobilen Geräts und Herstellerspezifikationen, die beim Hochladen eines Fotos auf eine Plattform geteilt werden.
- Die nächste Aufgabe bestand darin, dass die Teilnehmer/innen mit ihren Geräten nach dem nächstgelegenen italienischen Restaurant suchten. Diese Suche ermöglichte die Erfassung der Domänen, die die Smartphones ansteuerten (sowohl die sichtbaren als auch die unsichtbaren aus der Sicht der Benutzer/innen) und der Daten über die verwendete Suchmaschine, das Navigationstool oder den Browser.
- Am Ende des Besuchs erhielt jede/r TeilnehmerIn Informationen über die Menge der während seines Aufenthaltes von den verschiedenen Plattformen gesendeten / empfangenen Daten, die statistisch und visualisiert in Form verschiedener Diagramme dargestellt wurden. Das Ergebnis sollte motivieren, diverse Standardeinstellungen, Apps und die eigene Internetnutzung zu überdenken. Am Ende des Experiments wurden die Besucher/innen zudem gefragt, ob sie unsere Forschung durch das Ausfüllen eines Online-Fragebogens weiter unterstützen würden.

Der quasi-experimentelle Aufbau lieferte den Nachweis, dass personenbezogenen Daten von Dritten leicht verfolgt werden können, während der Online-Fragebogen Informationen über Verhalten, Zusammenhänge und das Bewusstsein für Datenaustauschprozesse der Teilnehmer/innen lieferte. Besucher/innen, die zum Ausfüllen des Fragebogens bereit waren, mussten eine Vereinbarung unterzeichnen, dass ihre Daten gespeichert und mit der Besucher-ID verknüpft werden.

6.2 Die wichtigsten Ergebnisse der Pilotstudie[2]

Die Befragten der Online-Umfrage (N= 102) waren überwiegend weiblich (73,8 %); 46,1 % hatten Matura o. Ä. und 32,4 % einen Universitäts- bzw. Hoch-

[1] Mangels Kontroll- bzw. Vergleichsgruppe handelt es sich um ein Quasi-Experiment (nicht um ein Experiment) (vgl. Bailey 1994: 236)

[2] Gesamtstudie unter: Atteneder, H. & B. Collini-Nocker (2018): Geomedia and privacy in context – Paradoxical behaviour or the unwitting sharing of geodata with digital platforms? In: Mediatization Studies (2), 17–48.

schulabschluss. Das Durchschnittsalter der Teilnehmer/innen betrug 29,38 Jahre (Perzentile: 25 => 21 Jahre; 75 => 32 Jahre). Zur allgemeinen Frage des App-Nutzungsverhaltens möchten wir auf folgende Punkte hinweisen: 88,2 % gaben an, regelmäßig Google Maps zu verwenden; 96,7 % dieser Gruppe gaben an, dass sie es für nützlich hielten, während 60 % der Nicht-Nutzer/innen es aus Gründen des Datenschutzes nicht verwendeten. Die am zweithäufigsten genutzte App-Kategorie war „Apps für den öffentlichen Verkehr" (83,3 %), gefolgt von Social Network Apps (78,4 %). Die häufigsten Gründe für die Nutzung von Social-Network-Apps waren „um informiert zu bleiben" (65 %), „weil Freunde sie nutzen" (63,8 %) und „Nützlichkeit" (56, 3%). Gefragt nach der eigenen Einschätzung, Datenschutzmanagement zu betreiben, gaben 44,9 % der Befragten an, sich nicht in der Lage zu fühlen, ihre Daten vor der Weitergabe und Nutzung durch Dritte zu schützen.

6.3 Hypothesentests:

Hypothese 1, die besagte, dass sich die Mehrheit der Menschen um den Schutz ihrer (Geo-)daten und um ihre Privatsphäre sorgten, aber dennoch Geomedien nutzten und damit ihre Daten preisgaben, wurde über zwei Indizes getestet. Diese Hypothese wurde teilweise unterstützt. Eine schwache bis moderate Korrelation zwischen den beiden Indizes trat auf ($p=0.13$; $r \leq 0.268$), allerdings mit keinem signifikanten Ergebnis ($p=0.161$) innerhalb der gegebenen Stichprobe (58 %). Wir konnten in unserer Studie also das „privacy-paradox", bezogen auf Geomedien nicht bestätigen. Je mehr unsere Testpersonen also über Datenschutz Bescheid wussten und sich um den Schutz ihrer Privatsphäre sorgten, desto restriktiver gingen sie mit der Freigabe ihrer Daten um. Zusätzlich gaben 45 % der Befragten an, dass sie Maßnahmen zum Schutz ihrer Privatsphäre im Internet ergriffen haben. Von dieser Gruppe gaben 93,5 % an, dass sie die Datenschutzeinstellungen für bestimmte Apps bewusst geändert und die „Opt-out"-Optionen in vollem Umfang genutzt haben. 65,2 % gaben an, dass sie bestimmte Anwendungen/Plattformen aus Datenschutzgründen niemals nutzen würden. 26,1 % nutzten einen verschlüsselten E-Mail-Dienst. Nur 17,4 % nutzten eine Suchmaschine, die das Suchverhalten nicht verfolgt. 50 % antworteten, dass die Ortungsfunktion auf ihrem Smartphone generell deaktiviert sei. 48 % antworteten, dass sie den Standortzugang für ihre Smartphone-Kamera deaktiviert hätten, während 27,5 % angaben, dass ihre Smartphone-Kamera zu den Diensten gehört, die einen permanenten Zugang zu ihrem Standort haben (18,6 % wussten nicht über ihre Einstellungen Bescheid). 25,5 % gaben an, dass sie ihren Standortverlauf normalerweise mit Google oder Apple teilten, 52,9 %, dass sie diesen nie teilen, und 15,7 % wussten es nicht. Zusammenfassend kann festgehalten werden, dass Geodatenschutzmanagement für wichtig erachtet wird, die Maßnahmen sich jedoch in dem von der jeweiligen Applikation vorgegebenem Rahmen bewegen.

Hypothese 2 testete kontextuelle Faktoren zur Standortfrei- und Datenweitergabe. Der Standort wird in verschiedenen Kontexten unterschiedlich gerne geteilt. 22,5 % teilen ihren Standort im Allgemeinen mit Familie und Freunden; 20,2 % teilen ihn mit Familie, Freunden und Partnern, wenn sie auf Reisen sind. 52,8 % antworteten, dass sie ihren Standort in keiner der gegebenen Situationen teilen würden.

Die Hypothese wurde für jede App-Kategorie separat getestet (Sightseeing, öffentlicher Nahverkehr, Wetter, Google Maps, Apple „Maps", Social Networking, Shopping, Fitness, Dating) und mit dem jeweiligen kontextuellen (und motivationalen) Nutzungsmuster abgeglichen:

- Nutzen $\chi2(9) = 83.015$, $p < 0.001$
- Beruflicher Kontext $\chi2(9) = 13.815$, $p < 0.129$
- relevante Informationen erhalten/informiert bleiben $\chi2(7) = 67.556$, $p < 0.001$
- aus Angst etwas zu verpassen $\chi2(4) = 22.515$, $p < 0.001$
- weil Freunde es benutzen $\chi2(9) = 191.333$, $p < 0.001$
- weil die Familie es verwendet $\chi2(9) = 63.895$, $p < 0.001$

Das Ergebnis ist statistisch signifikant. Obwohl 52,8 % der Teilnehmer antworteten, dass sie ihren Standort in „keiner der gegebenen Situationen" teilen, sind Motivation und Kontext entscheidend für das Verhalten der App-Nutzung.

Hypothese 3 prognostizierte, dass die Mehrheit der Menschen sich der kommerziellen Datenaustauschprozesse hinter der Nutzung von Geomedien bewusst sei, aber nicht in vollem Umfang. Die Hypothese wurde durch die Berechnung eines Indizes für „Bewusstsein für kommerzielle Datenaustauschprozesse" getestet. Dieser Index wurde dann anhand der Schwelle für „nicht in vollem Umfang" getestet. Die Hypothese wurde falsifiziert, weil 50 % der Menschen das volle Ausmaß der kommerziellen Datenaustauschprozesse kannten.

6.4 Ergebnisse des Quasi-Experiments:

79 Personen nahmen an unserem Quasi-Experiment teil, d. h. 79 Smartphones waren während der Testphase insgesamt mit unserem Research-Webservice ver-

bunden. 69 der Teilnehmer/innen konnten ein Selfie hochladen, so dass wir die Exif-Metadaten analysieren konnten. Aus nur 11 davon konnten wir den Standort (GPS-Daten) extrahieren, aber wir konnten Informationen über die am häufigsten verwendeten Smartphone-Marken, aktuelle Versionen von laufenden Betriebssystemen und verwendete Browser extrahieren. Insgesamt wurden während des Experiments 1,12 GB Datenmaterial hochgeladen. Während des gesamten Experiments riefen die Smartphones der Teilnehmer/innen (ohne deren Wissen) 3 916 Domains auf. Die fünf häufigsten (unwissentlich) geöffneten Domains waren www.google.com (359 Hits), connectivitycheck.gstatic.com (82 Hits), www.google.at (78 Hits), android.clients.google.com (56 Hits) und play.googleapis.com (53 Hits). Google APIs (Application Programming Interfaces) sind Google Analytics-Tools, die aus Perspektive der Nutzer/innen unsichtbar ausgeführt werden und Website-Nutzungsstatistiken für Google und seine Partner enthüllen. Betrachtet man nur die Second-Level-Domains, so ergibt sich folgendes Ranking: google.com (713 hits), apple.com (367 hits), googleapis.com (311 hits), gstatic.com (217 hits), google.at (138 hits), googleuser-content.com (123 hits) und icloud.com (108 hits).

Unseren Ergebnissen zufolge versuchen die Nutzer/innen entlang ihrer Möglichkeiten, und anhand kontextueller Faktoren, ihre Privatsphäre zu schützen und den bestmöglichen Kompromiss zwischen einem Eingriff in die Privatsphäre und größtmöglicher Bequemlichkeit zu finden, tun dies allerdings nur innerhalb des für sie sichtbaren Bereichs (durch Änderung der Privatsphäre-Einstellungen, Zurückhalten bestimmter Inhalte usw.). Der verborgene Teil von Datenweitergabeprozessen ist intransparent und unkontrollierbar. Dies wirft ein neues Licht auf das Paradoxon des Datenschutzes, da wir die faktische Unmöglichkeit einer vollständigen Kontrolle von Data Mining und Marketing, Aggregation, Filterung und Reorganisation berücksichtigen müssen. Selbst eine strikte Nichtnutzung bestimmter Services stellt keinen Schutz der Privatsphäre dar: Die AP (Associated Press) berichtete im August 2018, dass Google den Standortverlauf speichert, auch wenn dieser auf dem mobilen Gerät deaktiviert wurde (Nakashima 2018). Unter den Teilnehmerinnen und Teilnehmern unserer Studie ist Google Maps die am häufigsten genutzte App und mit 88,2 % das wichtigste Tool zur Navigation. Wenn wir diese Ergebnisse mit dem Ergebnis der von unserem Research-Webservice erhobenen Daten verknüpfen, können wir die enorme Rolle von Google demonstrieren. Google kann eindeutig als einer der dominanten Akteure und damit als Akteur der Internet-Oligopolie (Smyrnaios, 2018) identifiziert werden, da die fünf wichtigsten Second-Level-Domains zum gegenseitigen Informationsaustausch Google-Dienste waren. Da Geomedien die Kommunikation „kontextualisieren“ (Gryl & Jekel 2012: 22), „soziales Verhalten und zwischenmenschliche Kommunikation regeln“ (Lapenta 2011) und die Raumaneignung beeinflussen, ist die Dominanz eines Big Players aufgrund einer Einschränkung der Vielfalt zu kritisieren.

Die Teilnehmer/innen unserer Studie zeigten ein hohes Maß an Bewusstsein für die versteckten Datenweitergabeprozesse und die kommerziellen Ziele der Service-Anbieter. Generell ist anzunehmen, dass Teilnehmer/innen an der „Langen Nacht der Forschung“ als interessierter und kritischer gesehen werden müssen (Atteneder & Collini-Nocker, 2018). Dementsprechend hoch fielen die individuellen Initiativen zum Schutz der eigenen Privatsphäre aus. Auffällig ist die überdurchschnittlich hohe formale Bildung der Teilnehmer/innen, die zwar einerseits die Repräsentativität unserer Studie, also die möglichen Rückschlüsse auf die Gesamtbevölkerung schmälert, jedoch den vorsichtigen Schluss auf einen anderen Aspekt zulässt: Bildung und ein geschärftes Problembewusstsein fördert einen kritischen Umgang mit Geomedien. Insbesondere Bewusstseinsbildungsprozesse bei Kindern und Jugendlichen, die als „digital natives“ die am stärksten betroffene und umworbene Generation darstellen, können als wichtiges Instrument zur Förderung eines reflexiven Geomedienhandelns gesehen werden. Die Ergebnisse der Pilotstudie auf der „Langen Nacht der Forschung“ dienten als Grundlage für einen Workshop für Schüler/innen, der hier exemplarisch dargestellt werden soll.

7 Methoden und Ansätze für einen Workshop an Schulen

Zum Thema räumlicher Privatsphäre gibt es ausgearbeitete Lernumgebungen aus verschiedenen und auch häufig von Jugendlichen in Anspruch genommenen Bereichen. Dazu zählen beispielsweise Apps aus Skigebieten, die die individuelle Abfahrtsleistung des Skitages nachvollziehbar machen (vgl. Winkler et al. 2013) und sich somit hervorragend an Skikursen oder Skitagen thematisieren lassen – inklusive der ökonomischen Interessen der Anbieter/innen und individuellen Kontrollmöglichkeiten. Eine grundsätzlich ähnliche Unterrichtsumgebung legen Höhnle et al. (2013) vor. Für die räumliche Überwachung in der Stadt, wie sie auch durch Mobiltelefone gegeben ist, entwickelte Stark (2014) eine Unterrichtsumgebung, die sowohl auf die Stärken räumlicher Analyse, als auch auf die Schwächen hinsichtlich des Schutzes der Privatsphäre hinweist. Allerdings beruhen alle diese

Beispiele lediglich auf dem Tracking von Individuen, und lassen die Analyse weiterer Daten völlig außer Acht. Genau diese Schwäche will der hier vorgeschlagene Workshop umgehen.

7.1 Ablauf Workshop

Der hier vorgeschlagene Workshop-Ablauf wurde im universitären Kontext pilotiert und verbessert. Der dargestellte Ablauf und die Ergebnisse beziehen sich auf die Durchführung an der HLW (höheren Lehranstalt für wirtschaftliche Berufe) mit Schülerinnen und Schülern, in der Vertiefung „Mobile Endgeräte und Medien". Insgesamt haben 25 Schüler/innen der 4. Oberstufenklasse (12. Schulstufe) teilgenommen.

Für den Workshop wurden drei Unterrichtseinheiten bzw. je nach Möglichkeit ein ganzer Vormittag anberaumt, die inhaltlich, sowie zeitlich in Übereinkunft mit den jeweiligen Lehrpersonen ausgestaltet wurden. Der Workshop hat direkte Relevanz für die Fächer Geographie/Wirtschaftskunde und die Themen Datenschutz, Sicherheit im Netz bzw. privacymanagement vorbereitet. Der Workshop startete mit einem Kurzvortrag in Form eines Pecha-Kucha (Vortragsformat bei dem 20 Folien, die überwiegend Bildinhalte zeigen exakt 20 Sekunden aufgelegt werden), die in knapper Form die Datensammlungs- und Kommerzialisierungsstrategien der Unternehmen bzw. die algorithmischen Verarbeitungsprozesse der erhobenen Daten thematisierte. Insbesondere sollte eine Sensibilisierung in Hinblick auf eine mögliche Risikobewertung von Bürgerinnen und Bürgern

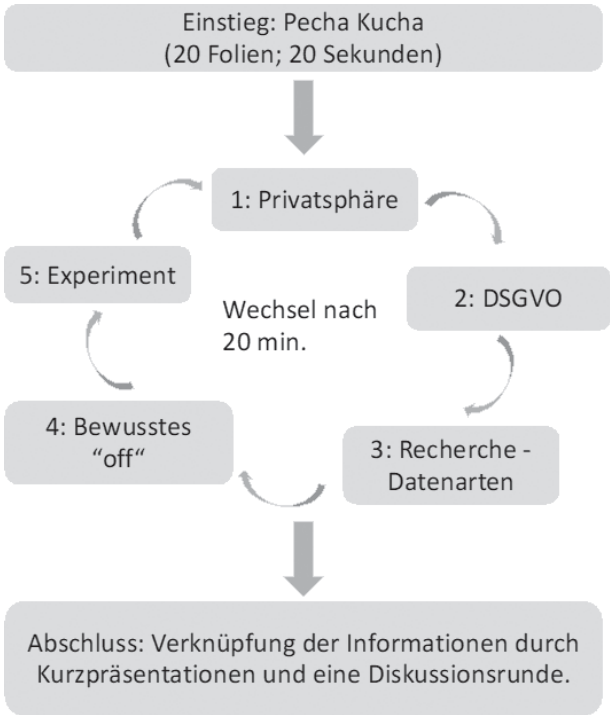


Abb. 3: Ablaufchart Workshop (eigene Darstellung)

stattfinden. Anschließend wurden die Schüler/innen in fünf Gruppen für einen Stationenbetrieb aufgeteilt. In Form eines Worldcafés mussten die Gruppen 1 bis 4 Aufgabenstellungen auf Flipcharts bearbeiten, während Gruppe 5 mit dem Experiment, analog zu dem zuvor beschriebenen Quasiexperiment, beschäftigt war. Im 20-minütigen Rhythmus wechselten die Gruppen und diskutierten und ergänzten auf den Flipcharts oder nahmen am Experiment teil. Für einen reibungslosen Ablauf blieb jeweils ein/e Schüler/in durchgehend bei den Flipchart-Stationen als Diskussionsleiter/in. Inhaltlich mussten die folgenden Bereiche bearbeitet werden:

1. „Was bedeutet für dich Privatsphäre?"
2. „Inwiefern betrifft dich die Datenschutzgrundverordnung?"
3. „Recherchiere: Was sind Metadaten? Was Verkehrsdaten und was sind Inhaltsdaten?"
4. „Gibt es Situationen in denen du dein Smartphone bewusst ausschaltest (oder den Flugmodus verwendest)? Aus welchen Gründen?"

Zur Beantwortung der Fragen war die Nutzung der eigenen Smartphones ausdrücklich erwünscht.

7.2 Ergebnisse und Empfehlungen

Die Schüler/innen zeigten großes Interesse an den Workshopthemen und arbeiteten konzentriert und aufmerksam an den Aufgabenstellungen. Durch die abschließenden Kurzpräsentationen und die sich daraus ergebenden Diskussionen konnten vonseiten der Workshop-Leiter/innen gezielt Nachfragen gestellt und so die Inhalte aufgearbeitet werden. Das Thema „Was bedeutet für dich Privatsphäre?" wurde von den Schülerinnen und Schülern sehr breit aufgefasst. Privatsphäre sowohl bezogen auf körperlicher Distanz („eine Armlänge Abstand"), als auch auf einen privaten eigenen Raum („eigenes Zimmer als Rückzugsort") wurde im Spannungsfeld der durch Geomedien entstehenden zunehmenden Verwischung einer privaten vs. öffentlichen Sphäre diskutiert. Ob und in welcher Weise eine Form von Privatsphäre gegeben wäre und wie sich damit das klassische Raumverständnis verändert, wenn die Schüler/innen, zum Beispiel, „always on" in den eigenen vier Wänden Geomedien nutzen, war eines der Themen. Artikuliert wurde auffallend stark die Wichtigkeit eines Rechts auf Privatsphäre und die Kontrolle über die eigenen Daten, was sich unter dem Begriff der informationellen Selbstbestimmung fassen ließe, wenngleich der Begriff von den Schülerinnen und Schülern nicht benutzt wurde. Kontextspezifische Handlungsmuster bezogen auf privacymanagement (bspw. ärztliche Schweigepflicht und ein stärkerer Schutz von Gesundheitsdaten vs. einer allgemeinen Akzeptanz von Überwachungskameras im öf-

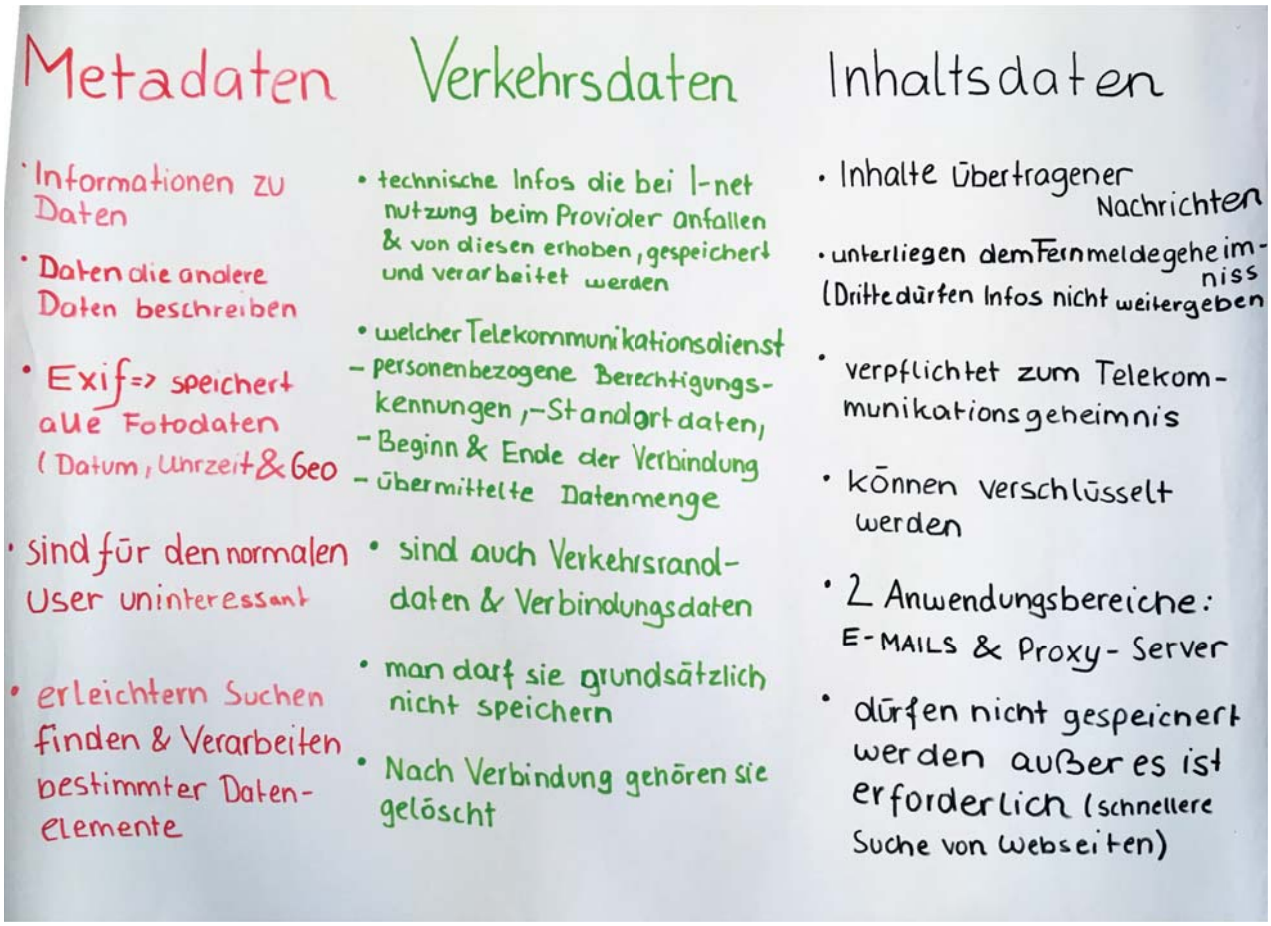


Abb. 4: „Ergebnis des Rechercheauftrags zu den verschiedenen Datenarten“. (Quelle: HLW, 12. Schulstufe)

fentlichen Raum) konnten eindeutig herausgearbeitet werden und der Rückbezug auf das Konzept der kontextuellen Integrität (Nissenbaum 2010) liegt nahe.

Der Themenblock 2 zur DSGVO lenkte die Aufmerksamkeit der Schüler/innen auf die rechtlichen Bestimmungen und deren Auswirkungen, deren genaue Inhalte vorerst recherchiert werden mussten. Die detaillierte Ausarbeitung zeigte, dass rechtliche Rahmenbedingungen in nahezu allen Lebensbereichen (Freizeitgestaltung, Arbeit, Reisen, Wahlverhalten, etc.) eine Rolle spielen und vor diesem Hintergrund konnten Pro und Kontraargumente für rechtliche Regulierung diskutiert werden.

Thema 3 bestand aus der Rechercheaufgabe zu Meta-, Verkehrs- und Inhaltsdaten. Die Schüler/innen konnten ihre Recherchekompetenzen unter Beweis stellen. Das Ergebnis war eine erstaunlich präzise Aufstellung der verschiedenen Datenarten (siehe Abb. 4). Dieses Grundverständnis diente als Diskussionsgrundlage für das Eisbergmodell von Debatin et al. (2009). Gezielte Nachfragen zu den Datenschutzstrategien der Schüler/innen zeigten, dass diese nur oberflächlich (bezogen auf Inhaltsdaten) stattfänden. In der Diskussion konnte außerdem herausgearbeitet werden, dass sich das Wissen der Schüler/innen zu den Kommerzialisierungsstrategien der großen Plattformen auf Third-Party Cookies von Amazon beschränkt und das Wissen über Vermarktungslogiken jenseits der zielgruppenspezifischen Werbung, etwa zur Risikobewertung nicht vorhanden ist. Insbesondere die spezifische Rolle von Geodaten in Prozessen des Data Mining und Marketing, der Aggregation, Filterung und Reorganisation war den Schülerinnen und Schülern nicht bewusst.

Themenblock 4 fragte nach den Situationen, in denen das Smartphone bewusst ausgeschaltet oder in den Flugmodus versetzt würde. Die Aussagen, gelistet nach Häufigkeit der Nennung ergeben ein eindeutiges Bild: das Smartphone wird überwiegend unfreiwillig ausgeschaltet! Bei einem leeren Akku (14 Nennungen), um Fehlfunktionen zu beheben – Restart (14 Nennungen), um Updates zu machen (8 Nennungen) und um Reparaturen durchführen zu lassen (6 Nennungen). Drei Personen gaben an, sie würden das Smartphone bei der Führerscheinprüfung ausschalten und zwei Personen schalten es regelmäßig in der Nacht aus um Störungen zu vermeiden. Wir können zusammenfassend festhalten, dass das Leben der befragten Schüler/innen *in* den Medien stattfindet, um Deuze (2012) zu zitieren. Abschließend stellten

wir den Schülerinnen und Schülern und Lehrpersonen die Ergebnisse des Experiments in aufbereiteter Form zur Verfügung. Unter Rückbezug auf die Themenblöcke 1 bis 4 konnten so abschließend die Datenweitergabeprozesse der jeweils eigenen Smartphones veranschaulicht werden.

8 Zusammenfassung und Ausblick

Dieser Beitrag behandelt die Frage, ob Smartphoneuser/innen über versteckte Datenweitergabeprozesse und zugrunde liegende Kommerzialisierungsstrategien diverser Internet-Plattformen Bescheid wissen und ihr Handeln dementsprechend anpassen. Insbesondere das Wissen über die spezielle Rolle von Geodaten in Szenarien des Datenmissbrauchs und der Verletzung der Privatsphäre sollte untersucht werden. Das klassische „privacy paradox", wie es Barnes (2006) attestiert konnte in diesem Setting nicht bestätigt werden. Das heißt eine Dichotomie zwischen dem Wissen über Datenweitergabeprozesse und den daraus folgenden Handlungen konnte nicht gefunden werden. Nutzer/innen unserer Studie versuchten entlang ihrer Möglichkeiten und anhand kontextueller Faktoren ihre Privatsphäre zu schützen, kratzen dabei jedoch nur an der Oberfläche. Die große Menge an unsichtbar geteilten Meta- und Verkehrsdaten konnte durch das Quasi-Experiment sichtbar gemacht werden. Hervorzuheben ist dabei, dass die Teilnehmer/innen unserer Pilotstudie eine überdurchschnittlich hohe formale Bildung aufwiesen, was einerseits eine Verallgemeinerung der Ergebnisse ausschließt, jedoch andererseits den Stellenwert von Bildung hervorhebt!

Subsummierend kann festgehalten werden, dass der Handlungsspielraum der Nutzer/innen durch die Geschäftsmodelle und Datenschutzrichtlinien der jeweiligen Plattformen determiniert wird. Es besteht also eine Kluft zwischen dem *potentiellen Handlungsspielraum* und dem *tatsächlichen Datenfluss*. Diese Kluft deutet auf ein ungleiches Machtgefälle zwischen Unternehmen, den Nutzerinnen und Nutzern und den politischen Entscheidungsträgerinnen und Entscheidungsträgern hin. Dass die Implikationen der Geodatenverarbeitung selbst für kritische und informierte Nutzer/innen letztlich unbekannt und nicht nachvollziehbar sind, lässt eine gesellschaftspolitische Dimension erahnen, die trotz DSGVO im Hinblick auf virtuelle Gruppen noch nicht hinreichend abgedeckt ist und dringend politischer und rechtlicher Ausgestaltung bedarf. So sollten beispielsweise Transparenz und Auskunftspflicht Bestandteil der neuen ePrivacy-Verordnung werden, wo bereits im Entwurf des Artikels 8 jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer/innen untersagt ist, sofern sie nicht, u. a. für die Durchführung oder Bereitstellung eines Dienstes, notwendig ist oder die Benutzer/innen eingewilligt haben (vgl. Europäisches Parlament & Europäischer Rat, 2017, p. 31). Tatsächlich gehen einige der Erwägungsgründe im Vorschlag bereits in diese Richtung und müssten unterstützt und erweitert werden. Der Schutz der Privatsphäre durch strenge Gesetze und starke vertrauenswürdige Institutionen wird in einer immer komplexer werdenden Technik- und Wirtschaftsumgebung unerlässlich. Der Trend zu einer vollständigen Abwälzung jeglicher Verantwortung auf die Individuen gemäß einer neoliberalen Deutungslogik soll hier nicht unterstützt werden.

Gleichzeitig zeigt die Arbeit mit den sogenannten „digital natives", dass das Verständnis von Privatsphäre im Wandel begriffen ist. Die Grenze zwischen „privat" und „öffentlich" verschwimmt zunehmend und klassische, dichotome Modelle verlieren an Aussagekraft. Ein neues Privatsphäre-Verständnis sollte sich weniger an Containerräumen wie häuslichen Begebenheiten oder Nationalstaaten orientieren, sondern vielmehr abhängig von Kontext, „Kommunikationsziel" und letztlich auch Beziehungsgeflecht, Transparenz und individuelle Kontrolle befördern.

Sensibilisierung und Bewusstseinsbildung ist ein erster wichtiger Schritt, um bestehende Kontroll- und Machtbeziehungen zwischen Nutzern und Nutzerinnen, Staat / Politik und Konzernen zu hinterfragen. Im zweiten Schritt könnten bottom-up Initiativen und meso-level Kollektive zu einer nachhaltigen Veränderung der strukturellen Rahmenbedingungen führen.

Auf Basis der bisherigen Ergebnisse mit Schülerinnen und Schülern und den Pretests im universitären Umfeld, glauben wir bestätigen zu können, dass der beschriebene Workshop erheblich zur Bewusstseinsbildung beitragen kann. Darüber hinaus schlagen wir vor, diesen Workshop auch mittels qualitativer Prä-/Post-Interviews zu evaluieren.

Aufgrund der bereits genannten Limitationen der vorgestellten Studie geht unsere Empfehlung zur Entwicklung weiterführender Projekte, Workshops und Lernumgebungen im Bereich, mit dem Ziel einer erhöhten Sensibilisierung für die ubiquitäre Geodatenerfassung und die zugrunde liegenden Geschäftsmodelle. Ziel soll dabei sein, bewusste, individuelle, kontextabhängige, Geoprivacymanagementstrategien für Schüler/innen anzuregen.

Dank

Die Veröffentlichung dieses Beitrags wurde vom Open Access Publikationsfonds der Universität Salzburg unterstützt.

Literatur

Abernathy, D. (2017): Using geodata & geolocation in the social sciences. SAGE, Los Angeles, London, New Delhi.

Acquisti, A. & R. Gross (2006): Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Danezis, G. & P. Golle (eds.): Privacy Enhancing Technologies. Berlin: Springer. S. 36–58.

Andrejevic, M. (2005): The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. In: Surveillance & Society 2. S. 479–497.

Arendt, H. (1958): The human condition. Univ. of Chicago Press, Chicago.

Atteneder, H., & Collini-Nocker, B. (2018). Geomedia and privacy in context. Paradoxical behaviour or the unwitting sharing of geodata with digital platforms? Mediatization Studies(2), 17–48. doi:10.17951/ms/2018.1.1. S. 17–68

Barnes, S. B. (2006): A privacy paradox: Social networking in the United States. In: First Monday 11.

Barreneche, C. & R. Wilken (2015): Platform specificity and the politics of location data extraction. In: European Journal of Cultural Studies 18. S. 497–513.

boyd, d. (2014): It‘s complicated: the social lives of networked teens. Yale Univ. Press, New Haven.

Bundesministerium für Bildung und Frauen (2014): Unterrichtsprinzip Medienerziehung – Grundsatzerlass. https://www.bmbf.gv.at/ministerium/rs/2012_04.pdf?51oyce (15.03.2019).

Christensen, M. (2014): Technology, Place and Mediatized Cosmopolitanism. In: Hepp, A. & F. Krotz (eds.): Mediatized Worlds: Culture and Society in a Media Age. Palgrave Macmillan UK, London. S. 159–173.

Christensen, M. & A. Jansson (2015): Complicit surveillance, interveillance, and the question of cosmopolitanism: Toward a phenomenological understanding of mediatization. In: New Media & Society 17. S. 1473–1491.

Christl, W. & S. Spiekermann (2016): Networks of control. facultas, Wien.

Debatin, B. (2011): Ethics, Privacy, and Self-Restraint in Social Networking. In: Trepte, S. & L. Reinecke (eds.): Privacy online: perspectives on privacy and self-disclosure in the social web. Springer, Berlin. S. 47–60.

Debatin, B., J. P. Lovejoy, A.-K. Horn & B. N. Hughes (2009): Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. In: Journal of Computer-Mediated Communication 15. S. 83–108.

DeCew, J. (2018): Privacy. In The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), ed. Zalta, E. N.

Deuze, M. (2012): Media Life. Polity Press, Cambridge.

Dienlin, T. & S. Trepte (2014): Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. In: European Journal of Social Psychology 45. S. 285–297.

Esri. (2012). Revealing the ‘Where’ of Business Intelligence using Location Analytics.

Europäisches Parlament, & Europäischer Rat. (2017). VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation). S. 1–40.

Fast, K., A. Jansson, J. Lindell, L. Ryan Bengtsson & M. Tesfahuney (2018a): Geomedia Studies. Spaces and Mobilities in Mediatized Worlds. Routledge, New York.

Fast, K., A. Jansson, M. Tesfahuney, L. Ryan Bengtsson & J. Lindell (2018b): Introduction to Geomedia Studies. In: Fast, K., A. Jansson, J. Lindell, L. Ryan Bengtsson & M. Tesfahuney (eds.): Geomedia Studies. Spaces and Mobilities in Mediatized Worlds. Routledge, New York. S. 1–17.

Fischer, F. (2010): Wertschöpfung 2.0: Neue Produktions- und Nutzungspraktiken auf dem Geoinformationsmarkt. In: GW-Unterricht 120. S. 30–46.

Fried, C. (1970): An Anatomy of Values. Harvard University Press, Cambridge.

Fuchs, C. (2011): Towards an alternative concept of privacy. In: Journal of Information, Communication & Ethics in Society 9. S. 220–237.

Geospatial Media and Communications (2018): GEOBUIZ. Geospatial Industry Outlook & Readiness Index. http://www.geobuiz.com/geobuiz-2018-report.html

Gryl, I. & T. Jekel (2012): Re-centring Geoinformation in Secondary Education: Toward a Spatial Citizenship Approach. In: Cartographica 47. S. 18–28.

Gryl, I., T. Jekel & K. Donert (2010): GI and Spatial Citizenship. In: Jekel, T., A. Koller, K. Donert & R. Vogler (eds.): Learning with Geoinformation V – Lernen mit Geoinformation V. Wichmann, Berlin. S. 2–11.

Habermas, J. (1962): Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Suhrkamp, Frankfurt am Main.

Haklay, M. (2017): Volunteered Geographic Information and Citizen Science. In: Kitchin, R., T. P. Lauriault & M. W. Wilson (eds.): Understanding spatial media. SAGE, Los Angeles. S. 127–135.

Höhnle, S., R. Hofmann & K. Pascal Miener (2013): „Ich weiß, wo du letzten Sommer gewesen bist!“ Locational privacy – Ein Thema für den Geographieunterricht. In: Gryl, I., T. Nehrdich & R. Vogler (eds.): geo@web: Springer Fachmedien Wiesbaden. S. 177–198.

Jansson, A. (2015): Interveillance: A New Culture of Recognition and Mediatization. In: Media and Communication 3. S. 81–90.

Kant, I. (1996): An Answer to the Question: What is Enlightenment? First Published 1798. In: Gregor, M. J. (eds.): Immanuel Kant. Practical Philosophy, Cambridge: University Press.

Klauser, F. & S. Widmer (2017): Surveillance and Control. In: Kitchin, R., T. P. Lauriault & M. W. Wilson

(eds.): Understanding spatial media, Los Angeles: Sage, 216–224.

Lapenta, F. (2011): Geomedia: on location-based media, the changing status of collective image production and the emergence of social navigation systems. In: Visual Studies 26, 14–24.

Leszczynski, A. (2017): Geoprivacy. In: Kitchin, R., T. P. Lauriault & M. W. Wilson (eds.): Understanding spatial media, Los Angeles: Sage, 235–244.

Lovink, G. (2016): Im Bann der Plattformen : Die nächste Runde der Netzkritik. Bielefeld: transcript.

Marwick, A. E. (2012): The Public Domain: Surveillance in Everyday Life. In: Surveillance & Society 9, 378–393.

Marwick, A. E. & d. boyd (2014): Networked privacy: How teenagers negotiate context in social media. In: New Media & Society 16, 1051–1067.

McQuire, S. (2016): Geomedia. Networked Cities and the Future of Public Space. Cambridge: Polity.

McStay, A. (2017): Privacy and the Media. London: SAGE Publications Ltd.

Murakami Wood, D. (2017): Spatial Profiling, Sorting and Prediction. In: Kitchin, R., T. P. Lauriault & M. W. Wilson (eds.): Understanding spatial media, Los Angeles: Sage, 225–234.

Murdock, G. (2017): Mediatisation and the Transformation of Capitalism: The Elephant in the Room. In: Javnost – The Public 24, 119–135.

Author. 2018. AP Exclusive: Google tracks your movements, like it or not. Associated Press.

Nissenbaum, H. (2010): Privacy in context. Stanford, Calif.: Stanford Law Books.

O'Neil, C. (2016): Weapons of Math Destruction. In: Discover 37, 50–55.

Pitney Bowes Inc. (2007): Location intelligence: the New Geography of Business.

Ricker, B. (2017): GIS. In: Kitchin, R., T. P. Lauriault & M. W. Wilson (eds.): Understanding spatial media, Los Angeles: Sage, 25–34.

Saker, M. (2016): Foursquare and identity: Checking-in and presenting the self through location. In: New Media & Society.

Schwartz, R. & G. R. Halegoua (2014): The spatial self: Location-based identity performance on social media. In: New Media & Society 17. S. 1643–1660.

Stark, H.-J. (2014): `See You`: A web-based approach for teaching about GPS. Map Analysis and Privacy to secondary school students. In: Jekel, T., E. Sanchez, I. Gryl, C. Juneau-Sion & J. Lyon (eds.): Learning and teaching with geomedia. Cambridge Scholars Publ., Newcastle upon Tyne. S. 151–163.

Steinmaurer, T. (2016): Permanent vernetzt. Zur Theorie und Geschichte der Mediatisierung. Springer, Wiesbaden.

Smyrnaios, N. (2018). Internet Oligopoly : The Corporate Takeover of Our Digital World. Bingley: Emerald Publishing Limited.

Thielmann, T. (2010): Locative Media and Mediated Localities: An Introduction to Media Geography. In: aether. the journal of media geography 5 A. S. 1–17.

Thielmann, T., L. van der Velden, F. Fischer & R. Vogler (2012): Dwelling in the Web: Towards a Googlization of Space. HIIG Discussion Paper Series No. 2012-03. SSRN: Social Science Research Network. http://ssrn.com/abstract=2151949 or http://dx.doi.org/10.2139/ssrn.2151949 (09.11.2015)

Westin, A. (1984): The Origins of Modern Claims to Privacy. In: Schoeman, F. D. (eds.): Philosophical dimensions of privacy. Cambridge Univ. Press, Cambridge. S. 56–74.

Wilken, R. (2018): The Necessity of Geomedia: Understanding the Significance of Location-Based Services and Data-Driven Platforms. In: Fast, K., A. Jansson, J. Lindell, L. Ryan Bengtsson & M. Tesfahuney (eds.): Geomedia Studies. Spaces and Mobilities in Mediatized Worlds. Routledge, New York. S. 21–40.

Winkler, B., A. Partl, K. Weilharter & K. Maier (2013): Einsatz der Applikation „Ski amadé Guide" im Unterricht. In: GW-Unterricht 130. S. 56–60.

Zuboff, S. (2015): Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. In: Journal of Information Technology 30. S. 75–89.

Zwick, D. & N. Dholakia (2001): Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right. In: Electronic Markets 11. S. 116–120.

Zwick, D. & N. Dholakia (2004): Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. In: Journal of Macromarketing 24. S. 31–43.

Material

Technische Umsetzung eines Personal Privacy Health Assessment

Die Analyse, wohin Daten von (speziell) Smartphones gesendet werden, ist eine zentrale Grundlage zur Ergreifung von Gegen- und Datenschutzmaßnahmen. Tatsächlich scheint die Datensammelwut von Apps trotz DSG 2018 in Österreich und DSGVO in Europa ungebrochen und immer mehr Programmiervereinfachungsangebote von (den großen) Plattformen erlauben die Integration und/oder Nutzung zur Analytics-Auswertung (oft mit dem Zusatz-Zauberwörtchen AI) im Austausch gegen (oft unbedacht personenbezogenen) Kunden- und Kundinnendaten. Aber selbst App-Entwickler, die einfach Push-Notifications implementieren wollen, können sich der vermeintlichen Attraktivität der Push-Services von Amazon, Apple, Google, Facebook, Samsung und vielen weiteren kaum entziehen.

Um die Daten, die von Anwendungen (Apps) am Smartphone ins Internet übertragen werden, zu analysieren, sind verschiedene Möglichkeiten implementierbar. Grundsätzlich, auch weil am einfachsten, ist die Messung der Verkehrsdaten zu bevorzugen, da diese meist keine personenbezogenen Daten beinhalten.

Bevor ein Smartphone Daten an einen Internet-Server senden kann, fragt er einen DNS Server nach der IP Adresse des Internet-Servers. Die IP Adresse des DNS Servers erfährt das Gerät zuvor bei der Anmeldung an ein WLAN. Der Anbieter des WLANs betreibt den DNS Server und kann die DNS Anfragen zwischenspeichern. Für die Auswertung werden aus den DNS Anfragen die angefragten Domänen der Internet-Server ausgelesen und angezeigt.

1. Phase: Manuelle Durchführung

Dazu wird ein Laptop/Notebook mit Linux installiert und als WLAN Access Point konfiguriert.
Sobald das Smartphone mit diesem WLAN verbunden ist, kann man nun jene App starten, an der man interessiert ist. Am Ende der Messung werden die DNS Anfragen dann nach Domänennamen gefiltert, sortiert und ohne Duplikate angezeigt. So lässt sich dann bei einer App herausfinden, ob sie zum Beispiel Facebook Analytics verwendet, weil dann beim Start der App Verbindungen zu facebook.com, fbcdn.com und ähnlich genannten Internet-Servern aufgebaut werden.

Für die Konfiguration des WLAN verwenden wir create_ap [1] welches man als Administrator mit „create_ap -m nat wlan0 eth0 meinWLAN meinKennwort“ startet. Dabei erzeugt create_ap ein WLAN mit dem Namen meinWLAN und dem Kennwort meinKennwort. Danach startet man die Messung mit „tcpdump -ni wlan0 -w dateiname.pcap port 53“. Damit werden die DNS Anfragen und DNS Antworten von der wlan0 Schnittstelle aufgezeichnet und in der Datei dateiname.pcap zwischenspeichert, die mit „tcpdump -xr dateiname.pcap wieder ausgelesen werden kann. Dabei werden die DNS Anfragen in der Form

```
15:15:38.843642 IP 192.168.1.2.39176 > 192.168.1.1.53: 34694+ A? facebook.com. (30)
15:15:38.856924 IP 192.168.1.1.53 > 192.168.1.2.39176: 34694 1/13/11 A 31.13.84.36 (506)
```

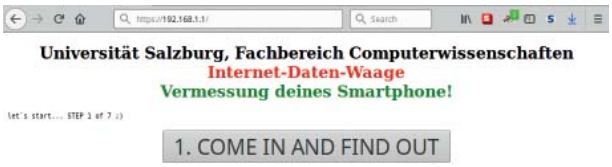
angezeigt. Die durch Leerzeichen getrennte erste Spalte zeigt dabei einen Zeitstempel, die zweite, dass es sich um IP handelt, die dritte Spalte zeigt die IP Adresse und Port des anfragenden Rechners (hier Smartphone) und die vierte Spalte die IP Adresse und Port des angefragten Rechners (hier DNS Server am WLAN Access Point), die weiteren Spalten dann die Anfrage bzw die Antwort.

Eine DNS Anfrage bzgl. facebook.com wird hier mit der IP Adresse 31.13.84.36 beantwortet, wobei wir ohnedies nur wissen wollen, dass facebook.com angefragt wurde. Indem man mit dem Unix-Befehl grep nach „A?“ sucht, lassen sich nur die DNS Anfragen heraus filtern. Die gefilterten Ergebnisse werden dann mit „sort -u“ zur leichteren Lesbarkeit sortiert und Duplikate herausgefiltert.

[1] https://github.com/oblique/create_ap/blob/master/create_ap

2. Phase: Halbautomatische Ausführung

Die Durchführung der Messungen kann weiter automatisiert werden, indem die einzelnen Befehle von Phase 1 über eine Website per Mausklick gestartet werden: im ersten Schritt wird das WLAN gestartet und auf der Webseite der Name des WLANs (die SSID) und das Kennwort angezeigt. Sobald das Smartphone verbunden ist, wird im zweiten Schritt die Messung gestartet. Nachdem die Messung mit Mausklick gestoppt wurde, wird im dritten Schritt die Auswertung gestartet und das Ergebnis dargestellt.



3. Phase: Halbautomatische Ausführung auf eigenem Gerät

Da die Verwendung des eigenen bzw. eines eigenen Notebooks für laufende Messungen dieser Art unpraktisch ist, verwendet man dafür einen preisgünstigen Einplatinencomputer. Der Einplatinencomputer muss dafür nur eine LAN-Schnittstelle für den Anschluss ans drahtgebundene Heimnetzwerk und WLAN für die Messung verfügen. Getestet wurde die Verwendung des Raspberry PI 3 Version B+, der sowohl über LAN als auch WLAN verfügt und etwa 35 € kostet.

Nach der Installation wird der Raspberry PI als WLAN Access Point entsprechend Phase 2 konfiguriert. Danach sollten noch die Einstellungen dahin gehend adaptiert werden, dass alle notwendigen Dienste beim Start des Raspberry PI automatisch gestartet werden, und schon steht ein eigenständiges und kostengünstiges Messgerät zur Verfügung.