 DOI: 10.17951/ms.2018.2.17-48

HELENA ATTENEDER

Department of Communication Studies, Center for ICT&S, University of Salzburg

helena.atteneder@sbg.ac.at

BERNHARD COLLINI-NOCKER

Department of Computer Sciences, Visual Computing and Multimedia Division, University of Salzburg

Bernhard.collini-nocker@sbg.ac.at

Geomedia and privacy in context. Paradoxical behavior or the unwitting sharing of geodata with digital platforms?

Abstract. The increasing pervasiveness of media in society implies the ubiquitous processes of geodata-capture and real-time feedback. The concept of Geomedia considers these developments and raises the questions of geoprivacy and corporate surveillance. The aim of this study was to investigate what kinds of geolocation data are shared wittingly or unwittingly, and in what contexts. Beyond that, we ask how much individuals know about the data-sharing processes and the underlying commercial logic, and how they act upon this knowledge (whether paradoxically or not). Our study was theoretically framed by contextual privacy (Nissenbaum 2011), because we assumed that a violation of privacy is perceived differently according to the context. The quasi-experimental design (using a WiFi-capture device) combined with a questionnaire revealed the participants' attitudes to, and awareness of, data sharing, and their understanding of geoprivacy and geomedia use. The main results show that people are aware of the underlying commercial logic, have privacy concerns and, strongly depending on contextual factors, their knowledge and capabilities, act upon this awareness. Finally, we show that smartphones covertly share a huge amount of meta and traffic data.

Keywords: privacy, geoprivacy, geomedia, privacy paradox, permanent spatial connectivity, ubiquitous geodata capturing, corporate surveillance, awareness

Introduction

Privacy concerns about online third-party tracking and monitoring as well as digital network behavior have received much attention in recent years due to the ubiquitous use of smartphones, the rise of the so-called "Big Five" (Google, Amazon, Microsoft, Facebook, and Apple – large platforms that permanently collect and monetize user data), and ongoing discussions about political and legal regulation strategies in the light of General Data Protection Regulation (GDPR). Among the whole range of collected sensor and usage data, geolocation is of particular interest as it reveals spatio-relational and spatio-temporal information about individuals (Wilken 2018). Location has gained importance across different disciplines and industries, and has become core to many business processes. Tech companies derive added value by combining, in unprecedented ways, the collection, aggregation, filtering and re-organization of networked personal data with *geolocational data* for even more precisely targeted marketing strategies and predictions, such as content customization and delivery (Estes 2016). In formulating new critical perspectives, including potential advantages and risks, several scholars use the term "geomedia" (Fast et al. 2018; McQuire 2016) to articulate the new societal conditions that arise through ubiquitous geodata capture, emphasizing the huge importance of media in the 21st century. Geomedia are indicative of dichotomies that appear to be inherent in internet technologies as a whole: they can be the "media of surveillance and control, of intrusion into intimacy" (Jekel et al. 2014, p. ix), media that influence political decision making and voting behavior, and the media of empowerment, democratization and engagement.

Given the omnipresent and widespread use of geomedia, we have to pose questions about their possible impacts on individuals and society, against the background of the shift from surveillance and intrusion into privacy exclusively realized by states and governments in the past to now the same by companies. This shift forms part of the economics of advanced capitalism (Murdock 2017), a driving force for technological development that shapes the possibilities of data-sharing. In this study, we focus on usage, privacy concerns and privacy management related to geolocational data at the level of the individual user, endeavoring to discover what types of geolocation data they unwittingly or deliberately share, and in what contexts. How much do individuals know about the data-sharing processes and the underlying commercial logic, and how do they act upon this knowledge? Although privacy concerns, behavior and attitudes are discussed widely in various disciplines, we are not aware of any study that evaluates the specific roles of geolocation and geomedia from a media and communication studies perspective. To theoretically frame the complex conditions under which people share or do not share data, we refer to Nissenbaum's contextual privacy approach (Nissenbaum 2010, p. 147), as she dismisses the public/private dichotomy and interprets privacy in relation to an appropriate flow of personal information (Nis-

senbaum 2010). Based on a combination of a questionnaire and a quasi-experimental setup, we show people's ideas about (locational) privacy in contrast to the data they actually, (un)wittingly, share by mobile device.

Living *in* Geomedia

The concept of mediatization is used to characterize media as one of the forces contributing to the constitution of societies nowadays. Mediatization is described as a "metaprocess" (Krotz 2007, 2017), from an institutional perspective (Altheide, Snow 1979; Hjarvard 2008, 2013), or as part of a social-constructivist tradition that recently introduced the term "deep mediatization" (Couldry, Hepp 2017; Hepp 2017). These approaches share the fact that they indicate that "modernity encompasses social and cultural changes in which more and more areas and forms of practice become saturated with and adapted to media technologies and institutions" (Jansson 2018, p. 2)[1]. Media (especially mass media) have always played an important role in structuring the fabric of society and public discourses. Currently, we have reached a point where ubiquitous smartphone use, datafication and artificial intelligence (especially machine learning algorithms) have penetrated people's final decision-making and action processes. Classical causal-linear models of mass communication no longer apply to these phenomena, and media and communication science theories that differentiated between producer/consumer, channel/content, interpersonal/mediated communication, real world/cyberspace, private/public no longer seem to fit, as these binary oppositions become blurred. An "almost complete mediatization of society seems a somewhat self-evident observation" (Deuze 2012, p. x), meaning that we do not live *with*, but *in* media. "Media are to us as water is to fish. This does not mean life is determined by media – it just suggests that whether we like it or not, every aspect of our lives takes place in media" (ibid.). For this reason, we suggest adhering to Deuze's definition of media, which captures them interchangeably as "information and communication technologies" and as "machines"; "[media] thus broadly conceived are any (symbolic or technological) systems that enable, structure or amplify communication between people" (Deuze 2012, p. xii). The shift from living *with* to living *in* media has some far-reaching consequences: media have become a necessary and unavoidable part of our lives; they are ubiquitous, pervasive (they cannot be switched off) and indeterminate (not finished or static); they act as platforms for communication to constitute and reproduce the world we live in (Deuze 2012, p. xi).

One aspect that made this densification of media possible is the "birth" of location-aware mobile devices. As they incorporate time *and* locational accuracy, they set the stage not only for a broad range of new applications but also for a whole range of new

[1] An extensive discussion of different approaches to mediatisation cannot be given here due to the focus on results.

possibilities for interaction. "The integration of the one-way GPS signal transmission into a two-way mobile communication system" (Abernathy 2017, p. 24) seems a small technological advance, but in fact it heralds a new era of mapping, connectivity, navigation, seeking of friends in places nearby, "checking in", observation and communication. Location-awareness has infiltrated a broad range of sectors and industries (healthcare, automobile, transport, education, banking, entertainment, tourism, government, etc.), and according to Wilken (2018) we now experience the seamless integration (if one unintended by users) of *location* with *services*, and (social) *networks*. This "ubiquitous geodata capture" (Wilken 2018, p. 26) marks the "third generation" (ibid.) of geodata services and platforms, where location has become vital for operation and service at all levels. This analysis not only applies to "native" third-generation services (like Uber), but also to established search and social media companies (such as Google and Facebook) that have effectively become "third-generation" location-based service platforms, insofar as they have reshaped their operations by ubiquitous geodata capture (Wilken 2018, p. 26). These services and platforms capture and circulate "geodata at a scale, speed and level of complexity that is markedly different from earlier incarnations of similar services" (Wilken 2018, p. 29).

In addressing these new conditions, several scholars introduced the term "geomedia" (Fast et al. 2018; McQuire 2016), which takes into consideration technological[2] and social change, critically addressing this permanent *spatial* connectivity.[3] Following a broader definition, geomedia "includes all representations of space, covering a wide range of outputs from verbal description to visualization. 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, p. 22). In his critical analysis, Lapenta (2011) argues that geomedia "regulate social behaviour and interpersonal communications, coordinate social interactions and organise the production and exchange of the founding immaterial commodities constitutive of these immaterial spaces" (Lapenta 2011, p. 22).

As Lapenta refers only to the technological aspects of geomedia, McQuire (2016) develops a much broader understanding of geomedia, placing far greater emphasis on urban conditions and including social change. "Geomedia is a concept that crystallizes at the intersection of four related trajectories: convergence, ubiquity, location-awareness and real-time feedback" (McQuire 2016, p. 2). Ubiquity refers to the omnipresence of mobile, embedded and connected media devices, available anywhere, anytime, even on the move; these devices converge increasingly with each other through the fusion of technologies, genres and institutions. Location-awareness

[2] Referring to a certain set of technological conditions. For details of this technological aspect, see Ricker (2017).

[3] "permanent connectivity" is used by Steinmaurer (2014) to describe a new type of communication (dispositive), defined by a new status of individual integration into the technological infrastructures of digital networks.

means that information is adapted to the user's location and mobility, while real-time feedback refers to the many-to-many flows of (locational) information in which the time between an event and its media presence is shrunk almost to zero, "supporting novel experiences of social simultaneity" (McQuire 2016, p. 4).

The possible implications of geomedia range from potential empowerment, activism (for example "smart mobs" (Rheingold 2002) and civic engagement (Gryl, Jekel 2012; Gryl, Jekel, Donert 2010; Haklay 2017) to intrusion into privacy and surveillance (Klauser, Widmer 2017; Leszczynski 2017; Murakami Wood 2017). If we want to analyze the impacts and importance of these "third-generation data-driven social, search, and analytics platforms" (Wilken 2018, p. 35) and formulate new critical perspectives, then the concept of geomedia, as presented in this chapter, can be seen as a "robust and productive framework" (ibid.)!

Geomedia and corporate surveillance

Geolocation has become not only an integral part of everyday smartphone experience and of changing appropriations and perceptions of space (Thielmann et al. 2012), but also "a necessary part of the technological developments and the corporate arrangements that underpin them (business deals, monetization strategies, platform-specific data extraction methods, algorithmic sorting, etc.)" (Wilken 2018, p. 21). The need to take into consideration these economic and socio-technical transformation processes underlines the necessity for academic debates on geomedia usage, behavioral patterns and privacy management. Geomedia structure communication spatially, but often in an unpredicted way, or in one that is unforeseeable and invisible to the user. Besides police and secret service work, it is applied most often in a commercial context. For example, pausing in front of a shoe-shop window, say, with your location-enabled smartphone in your pocket, without even actively using the phone, could reveal things of commercial interest to the Big Five (or others), even if you have never actively searched for shoes on shopping platforms.

The rising interest in geocoded data and their use in the mainstream market is reflected in the growth of the geospatial industry, which is projected to increase by a further 13.6% by the year 2020 (Geospatial Media and Communications 2018, p. 4). Using geocoded data is profitable for businesses in two ways: selling the geocoded data and creating new services out of the data to collect even more geocoded data. This has led to a change in the geoinformation market from one of corporate clients to a demand-driven mass market (Fischer 2010, p. 30). It is not only the world's leading software producer for GIS, Esri,[4] that stands to benefit from location intelli-

[4] Whitepaper on how to use location intelligence to maximize the Value of BI: https://www.esri.com/~/media/files/pdfs/library/whitepapers/pdfs/using-location-intelligence.pdf

gence;[5] even the core areas of popular internet use, dominated by "the Big Five" "Google in search; Facebook in social media; Amazon in online retailing; and Apple and Microsoft in personal computing;" (Murdock 2017, p. 123) are being reshaped by ubiquitous geodata capture. They "are at the heart of the emerging general economy of advanced capitalism" (Murdock 2017, p. 123), and collecting and trading users' personal data is the core of their business model. Murdock (2017, p. 130) suggests that one should analyze the dynamics of "deep capitalism" rather than those of "deep mediatization". These processes widely determine our everyday habits within the framework of mobile-network-technologies through (machine learning) algorithms and make corporate surveillance more precise. On an individual level, "new performances of self and re-inscriptions of the body in place and space" (Schwartz, Halegoua 2014, p. 1656), called the "spatial self" (Schwartz & Halegoua, 2014) arise; so too do new forms of identity-management (Saker 2016), self-surveillance, competition with others, and "watching one another", called "lateral surveillance"; (Andrejevic 2005). Individuals "[look] at [their] own content through other people's eyes" – social surveillance (Marwick, 2012), or "[control] one another" – interveillance (Jansson 2015), defined as the "social embeddedness of contemporary surveillance processes, typically governed by commercial forces, while at the same time recognizing the non-hierarchical and non-systematic nature of most social monitoring processes occurring in everyday life" (Christensen, Jansson, 2015; Jansson 2015, p. 81).

We assume that big platforms derive benefits from these developments in three ways: (1) information is collected regarding individual preferences, location and behavior, and (2) can be connected to individual networks of the (control-)relationships that emerge from interveillance; and (3) the collected data can be merged with data for virtual groups worldwide (i.e. groups of people with similar profiles). Subjects and their social and spatial behavior become controllable and predictable. Geomedia can therefore be seen as "progressing" as a close web of surveillance. Corporate surveillance is no longer just about targeted marketing. Furthermore, the creation of ever-more precise virtual groups can be used for risk-evaluation of citizens. These evaluations can be sold, for example to financial institutions to support decisions for awarding loans (O'Neil 2016), to health insurance companies to determine insurance premiums, to employers' associations to inform decisions regarding employment (such as salary and working hours), or to predict ex-criminals' reoffending rates. Most importantly of all, political decisions and knowledge of political opinions, which can be revealed easily, could, depending on the type of state, be misused. Geomedia therefore raise questions of "inclusion and exclusion, empowerment and exploitation, justice and injustice, equality and inequality" as

[5] Whitepaper from Pitney Bowes on „Location Intelligence: The New Geography of Business": http://media.govtech.net/RC_PITNEYBOWES/BusinessWeek.pdf

the "'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. 2018).

Geomedia privacy

Concepts of privacy that clearly distinguish between the private (associated with family, private households, intimacy) and the public sphere (communicative networks to foster the formation of public opinion), as found in ancient Greek literature (Aristotle) and later in the works of Habermas (1962) or Arendt (1958), must be revised as these two spheres become blurred and distorted by processes of advanced geo-digitalization. The extensive use of geomedia challenges these two-sphere-concepts. Individual spatial information (especially connected to a time stamp) is particularly sensitive with respect to the possible disclosure of personally identifying information (PII). Explained briefly, geolocation data are "(1) distributed (occur across multiple devices, applications and services), (2) platform-independent (data flow easily across platforms, services and devices) and (3) indiscriminate (involve potentially all individuals)" (Leszczynski 2017, p. 237). In this context, the need for a new understanding of privacy is raised by the "commercialization 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, p. 235).

While the historical and cultural notions of privacy vary widely and do not consistently estimate privacy desirable[6], we want to use it as a meaningful and valuable concept – as a major element of functioning democracies. Democracies "(or governance for the people by their elected representatives) innately value privacy because it promotes free development of the self, nonconformity, diversity of views, new ideas and opportunities to enjoy intimacy without unwanted scrutiny" (McStay 2017, p. 15), against negative accounts of privacy, based on seclusion and hiding, we want to condense it as autonomy, self-determination, voluntariness, free choice and responsibility for these choices (McStay 2017, p. 20). This follows Kant's understanding of these conditions, together with freedom being the basis of a social and moral life (Kant 1996). Based on Kant's notions of privacy, Fried (1970) characterizes privacy as the necessary condition for love, friendship and trust that "allows one the freedom to define one's relations with others and to define oneself. In this way, privacy is also closely connected with respect and self-respect" (DeCew 2018). Concerning digital network technologies, we also make privacy-decisions on behalf of others (p.e. sharing pictures and information about others or tagging a person). Therefore,

[6] For details see McStay (2017, pp. 11–24)

privacy has a collective character that is based on interactions with others (McStay 2017, p. 21). As Nissenbaum (2010) points out, privacy is more than the control of how much about ourselves we reveal to others, as stated by (Westin 1984). Moreover, the privacy and identity management strategies are dependent on contextual aspects. The normative concept of contextual integrity proposed by Nissenbaum (2010) looks at various information processes in various contexts. In an economic framework, a violation of privacy is caused differently in friendship-like relationships than in professional ones. "Given the power of companies in the capitalist economy, economic privacy needs to be contextualized in a way that protects consumers and workers from capitalist control and at the same time makes corporate interests and corporate power transparent" (Fuchs 2011, p. 232). From the perspective of the individual, the right to privacy "is neither a right to secrecy nor a right to control but a right to the appropriate flow of personal information" (Nissenbaum 2010, p. 127), and what is seen as appropriate is a normative distinction that involves the intersection of three aspects: actors, realm/space and information. When these norms are contravened, we experience a violation of privacy, here labelled a "violation of contextual integrity" (Nissenbaum 2010, p. 127). "At the level of politics, this requires governments to treat people with respect and dignity […]. The importance of liberal philosophy becomes clearer when we recognise that this holds sway over comprehension of human rights and the ethics that drive western law" (McStay 2017, p. 20). From a legal perspective, there are two different aspects (Zwick, Dholakia, 2001):

1) Privacy as a basic human need, and as a civil and human right (Debatin 2011), vs. privacy as a commodity or private property (discussed from a critical angle by (Fuchs 2011));

2) privacy regulation by Government vs. Self-regulation.

Different countries have developed different strategies. Whereas the EU legislation defines privacy as a basic human right and has established stronger legal regulation, in the US, privacy is equal to private property and seen as a commodity (Zwick, Dholakia 2001, p. 120). Companies with a transnational reach challenge these two concepts, and the efficacy of the recent attempt by the EU to reinforce legal regulation through the GDPR has still to be proved.

Self-disclosure, hidden data-sharing processes and privacy management

On the individual level, strategies for managing privacy and identity, according to Zwick and Dholakia (2004), are dependent on the accuracy and amount of personal Information revealed.

This model (Figure 1) gives the impression that the amount and accuracy of personal information is visible, controllable and manageable by the users themselves. It doesn't consider the hidden layers of the data-sharing processes.

		Accuracy of Personal Information Externalized	
		High	Low
Amount of Personal Information Externalized	High	Identifiability	Anonymity/ Pseudonymity
	Low	Confidentiality	Secrecy

Fig. 1: Four tactics of privacy and identity management (Zwick, Dholakia 2004)

With reference to social networking sites, Debatin (2011) identifies several privacy risks that users agree to when posting on sites, and plots them in two dimensions: a horizontal axis for social interaction among users (including cyberstalking, harassment, reputation damage, but also representation through profiles), exemplified metaphorically as the *visible* tip of the iceberg, and a vertical axis for data collected (systematic collection, aggregation and use of data by the networking company, data miners and government agencies, third-party tracking and monitoring), represented by the much larger submerged, *invisible* part of the iceberg (Debatin 2011, p. 4). Several other authors have investigated that many users are not even aware of the excessive data-sharing processes and pervasive monitoring of online and mobile platforms (Christensen 2014; Christensen, Jansson 2015).

There are numerous studies concerning the role of knowledge of data-sharing processes, privacy concerns and self-disclosure. boyd (2014) and Marwick and boyd (2014) showed that teenagers do not act carelessly on public networked spaces, but they cannot, despite privacy strategies, sufficiently control the information flows, an outcome that reveals how their technical skills are inadequate for the protection of privacy. A study on Facebook and other social network sites conducted by Acquisti and Gross (2006, p. 21) documented significant dichotomies between specific privacy concerns and actual information-revelation behavior. Although this study only examines student behavior, it provides evidence for the "privacy paradox" (Barnes 2006). Several other studies have demonstrated the existence of this paradox, flagging a gap between privacy concerns and action (for an overview see Dienlin and Trepte (2014, p. 294)), and a few studies indicate privacy paradoxes that can be explained to a certain degree (Debatin et al. 2009).

An in-depth social-psychological analysis of privacy attitudes and privacy behavior by Dienlin and Trepte (2014) offers a more complex picture. They distinguish between privacy concerns and privacy attitudes, and differentiate various privacy dimensions (informational, social and psychological), showing that "privacy behaviors are not paradoxical in nature but […] based on distinct privacy attitudes" (Dienlin & Trepte 2014, p. 295).

To bring the discussion back to everyday geomedia practices that are "characterised by extensive, real-time geosurveillance and the networked data and device ecologies" (Leszczynski 2017, p. 242), the link between privacy concerns (including knowledge on data-sharing processes and of the underlying commercial logic) and behavior cannot be described in a straightforward fashion. Quite the contrary: the contexts of data-sharing processes, economics and socio-technical transformation processes as well as the user's sociodemographic status all influence the appropriation of geomedia. The aim of this study was to investigate the specific roles of geomedia within this complex field.

Approach

In the first part of the paper we laid out the multifaceted nature of geomedia privacy management. It is with this aim in view that we posed the following research questions:

1. What kinds of traffic and metadata are shared unwittingly if the smartphone is connected to a WiFi spot?
   a. Of these, which are georeferenced?
   b. What are the specific contexts in which people would normally share or refuse to share these data?

There are different types of geodata (absolute location, relative location, (un)structured geodata) (Abernathy, 2017) that are received/gathered differently. Most commonly the receiving/gathering is carried out via an A-GPS – a GPS sensor assisted by WiFi positioning aand the triangulation of mobile radio cells, or it comes as data that is shared as part of the Exif data. Sharing (by the user with third parties) takes place actively (for example via WhatsApp, or by giving certain apps location access), or inadvertently (by having switched on location access, so Google's location API extracts information in the background on a continuous basis to push geo-targeted content – known as "geofencing" (Barreneche, Wilken 2015)).

As far as possible, we tried to determine the "precise nature" of this sharing of geodata.

1. How much do individuals know about data-sharing processes and the underlying commercial logic?
2. How do people act in light of this knowledge?

Our hypotheses were as follow:

Hypothesis 1 (H1):

The majority of people do care about the protection and control of geolocation data flows (even if in a loose and generally imprecise manner), but nevertheless share data using geomedia.

Hypothesis 2 (H2):

The amount and precise nature of the geodata shared depends on contextual factors.

We tested the following contexts and reasons for using geomedia and sharing geodata despite privacy concerns:

- Peer pressure
- Work pressure
- Fear of missing out
- Lack of knowledge
- "Careless" use (because "everybody uses the technology"; because of "not having anything to hide")
- Trade-off: convenience (service) vs. tracing

Hypothesis 3 (H3):

The majority of people are aware of commercial data-sharing processes behind geomedia use, but not of their full extent.

Methods

The entire study was carried out in the context of the Austrian "Long Night of Research" ("Lange Nacht der Forschung") at the University of Salzburg on 13 April 2018, during which our project maintained a stand informing interested people about geolocation data-sharing processes.

Using a combination of online questionnaire and quasi-experimental design (due to the lack of a control group / comparison group) (Bailey, 1994, p. 236), we examined people's knowledge concerning how their geolocation data is shared, wittingly or unwittingly, enquired about their day-to-day behavior regarding shared data, and examined their concepts of privacy. The particular nature of this project was, firstly, that it has a clear educational and informative aim, and that, secondly, it is used to foster academic knowledge.

The whole study was pre-tested in a university context. According to the findings of the pretest, questionnaire and quasi-experimental setup were improved in an iterative process. The procedure itself began with welcoming the visitors, typically families and groups of friends and/or students. In order to achieve maximum anonymity, no personal details were taken without consent, and the utmost care was taken to eliminate personally identifying information (PII). The participants were divided into groups of 2–6 people to guarantee anonymity, and led through the whole quasi-experimental

process. In the first step, they were asked to connect their smartphones to a randomly generated SSID (service set identifier) and were given a twelve digit passcode and a randomly generated four-digit Visitor ID. were given a four-digit passcode, which in turn randomly generated a Visitor ID. As soon as all the smartphones of a group were connected to our WiFi research device (to capture meta and traffic data), the participants were asked to take a selfie and to "share" (i.e. upload) it to a web service (operated by us). With this step, we were able to demonstrate the richness of the meta-information (metadata) included as Exif (Exchangeable Image File Format), such as GNSS-coordinates, type of mobile device, and manufacturer specifications, that are shared when a photo is uploaded onto a platform. The next task was for participants to use their devices to search for the nearest Italian restaurant. This search allowed the collection of the domains the smartphones targeted (both the visible and invisible ones from a users' perspective) and data about the search engine, navigation tool or browser being used.

At the end of their visit, each participant received information about the amount of data sent to/received from the various platforms during their stay, which was presented statistically (i.e. visualized) in the form of various diagrams intended to help motivate them to reconsider their default settings, apps and internet usage. The visitors were then asked whether they would support our research further by completing an online questionnaire (see appendix).

The quasi-experimental setup provided people with evidence that their personal data could be tracked easily by third parties, while the online questionnaire collected data regarding behavior, contexts and awareness of data-sharing processes. Visitors who were willing to participate were required to sign an agreement that their data would be kept and linked to the VisitorID. If they declined, the linkage between Visitor ID and recorded data was deleted.

Several limitations to the current study should be pointed out. First, the data was captured using a quasi-experimental design and cannot therefore be evaluated against a control group. The behavior captured only shows tendencies in an artificial context ("The Long Night of Research"), which may have encouraged people to give away data more freely. As the study was carried out in the context of a particular event, it cannot be repeated.

Second, the results of the questionnaire rely on interpretations of assumed behavior based on the respondents' self-reports: their actual day-to-day actions could not be monitored in this setup. We should also point out that answers regarding the importance of privacy may have been given in what was perceived to be a socially desirable way.

Finally, participation in our study was self-selecting and voluntary, and resulted in a voluntary sample with an unpredictable "n" (number of participants). Visitors to "The Long Night of Research" may in general be more highly educated, and more interested and critical than the average citizen.

Results

Quantitative online survey

The online survey respondents (n= 102) were predominantly female (73.8%); 46.1% had a higher school certificate or held a university degree (32.4%). The mean age of participants was 29.38 (percentiles: 25 => 21 years; 75 => 32 years). For the general question of app-usage behavior, we would like to draw attention to the following points (from Figure 2): 88.2% said they used Google maps; 96.7% of this group gave their reason as finding it useful, whereas 60% of the non-users did not use it for privacy protection reasons. The second most frequently used type of app were "apps for public transport" (83.3%), followed by social network apps (78.4%). The most common reasons for using social network apps were "to stay informed" (65%), "because friends use them" (63.8%) and "usefulness" (56.3%). Only 7.8% of the respondents said that they used dating apps.

		Reasons for usage (multiple choice)							Reasons for non-use (multiple choice)		
	Use (%)	Useful	Work	Stay informed	Fear of missing out	Because Friends use	Because Family use	**Don't use (%)**	Not interested	Don't know apps	Privacy protection reasons
Sightseeing apps	**39.2**	87.5	7.5	27.5	-	7.5	5.0	**60.8**	54.8	51.6	21.0
Public transport apps	**83.3**	92.9	12.9	28.2	-	4.7	3.5	**15.7**	37.5	50.0	18.8
Weather apps	**68.6**	85.7	10.0	50.0	-	1.4	2.9	**30.4**	87.1	9.7	12.9
Google Maps	**88.2**	96.7	16.7	-	-	5.6	4.4	**9.8**	60	20	60
apple "Maps"	**19.6**	95.0	10.0	-	-	0.0	0.0	**78.4**	37.5	61.3	3.8
Social Network apps	**78.4**	56.3	12.5	65.0	22.5	63.8	30.0	**19.6**	55.0	20.0	55.0
Shopping apps	**26.5**	100.0	3.7	22.2	0.0	3.7	3.7	**70.6**	91.7	6.9	13.9
Fitness apps	**31.4**	90.6	0.0	6.3	0.0	3.1	3.1	**64.7**	84.8	9.1	21.2
Dating apps	**7.8**	75.0	0.0	0.0	0.0	25.0	0.0	**88.2**	92.2	8.9	13.3
Delivery service apps	**22.5**	100.0	0.0	4.3	0.0	4.3	4.3	**73.5**	88.0	13.3	8.0

Fig. 2: digital application usage patterns

On a scale of 1 (fully agree) to 5 (completely disagree), 44.9% of respondents chose 1 or 2, meaning that they didn't feel able to protect their user-data from being shared and used.

Hypothesis tests

H1 predicted that the majority of people cared about the protection and control of geolocation data flows, but nevertheless shared data using geomedia. The hypothesis was tested by calculating an index for "care about the protection and control of geolocation data flows" and one for "share data using geomedia". This hypothesis was partially supported. A weak to moderate correlation between the two indices occurred (p=0.13; r0.268), though the hypothesis ("people would care about data protection but despite shared geodata") had no significant result (p=0.161) within the given sample (58%). We can state that the more people care about data protection and control of geolocation data flows, the less they share data using geomedia. 45% of the respondents said that they took measures to protect their privacy on the internet. Of this group, 93.5% said that they intentionally changed the privacy settings on certain apps and made full use of "opt-out" options. 65.2% said that they never used certain apps/platforms for privacy reasons. 26.1% used an encrypted email service. Only 17.4% used a search engine that did not track search behavior. 50% stated that the locating function on their smartphone was generally disabled. 48% stated that they disabled location access for their smartphone camera, whereas 27.5% stated that their smartphone camera was amongst those services that had permanent access to their location (18.6% didn't know about their settings). 25.5% said that they usually shared their location history with Google or Apple, 52.9% that they did not, and 15.7% did not know.

H2 predicted that the amount and precise nature of the geodata shared depended on contextual factors. Location is shared differently in different contexts. 22.5% generally shared their location with family and friends; 20.2% shared it with family, friends and partners when they were travelling; and 52.8% responded that they did not share their location in any of the given situations.

	Yes (%)
I normally share my location with my family/partner so that they know exactly who is where.	22.5
I usually share my location with friends (e.g. to arrange an exact meeting place)	19.1
When sharing pictures, I usually share my location intentionally (using GPS)	19.1
Within my professional network, I am required to share my current location	1.1
I share my location with my family/friends/partner when I'm away travelling	20.2
I share my current routes and performance when doing sports (e.g. running, hiking, etc.)	12.4
In none of the given situations	52.8

Fig. 3: "contextual factors" (multiple choice)

The hypothesis was tested for each app category separately (sightseeing, public transport, weather, Google Maps, Apple "maps", social networking, shopping, fitness, dating) with the contextual (and motivational) usage pattern:

Usefulness, $\chi2(9) = 83.015$, $p < 0.001$

Work, $\chi2(9) = 13.815$, $p < 0.129$

Relevant information/stay informed, $\chi2(7) = 67.556$, $p < 0.001$

Fear of missing out, $\chi2(4) = 22.515$, $p < 0.001$

Friends use it, $\chi2(9) = 191.333$, $p < 0.001$

Family use it, $\chi2(9) = 63.895$, $p < 0.001$

The result is statistically significant. Although 52.8% of participants answered that they shared their location in "none of the given situations", motivation and precise context matter in app-usage behavior.

H3 predicted that the majority of people were aware of commercial data-sharing processes behind geomedia use, but not their full extent. The hypothesis was tested by calculating an index for the "awareness of commercial data-sharing processes". This index was then tested against the threshold for "not to their full extent". The hypothesis was falsified because 50% of the people were aware of the full extent of commercial data-sharing processes.

The Quasi-experiment

A total of 79 people participated in our quasi-experiment (79 smartphones connected to our research web service). 69 of the participants managed to upload a selfie, so we were able to analyze the Exif metadata. It was possible to extract the location (GPS data) from only 11 of these, but we were able to extract information about the most frequently used smartphone brands, current versions of running operating systems and browsers used. In total 1.12 GB were uploaded. In the course of the whole experiment, the participants' smartphones made 3,916 valid domain name queries without their owners knowing it. The five most frequent (unwittingly) opened domains were www.google.com (359 hits), connectivitycheck.gstatic.com (82 hits), www.google.at (78 hits), android.clients.google.com (56 hits), and play.googleapis.com (53 hits). Google APIs (application programming interfaces) are google analytics tools that run invisibly (for the user) and reveal website-usage statistics to google and its affiliates. Considering the second-level domains only, the ranking was as follows: google.com (713 hits), apple.com (367 hits), googleapis.com (311 hits each), gstatic.com (217 hits), google.at (138 hits), googleuser-content.com (123 hits) and icloud.com (108 hits).

The information about the massive amount of data that is shared by a smartphone, as soon as it is connected to WiFi, while users are entangled in everyday geomedia usage, was presented to the participants visually in the form of various diagrams and should help motivate them to reconsider their default settings, apps and internet usage.

Discussion /Conclusion

The results of the online questionnaire indicated that there was a weak to moderate correlation between the indices "care about protection and control of geolocation data flows" and "share of data using geomedia" (with a statistically non-significant result). Therefore, the hypothesis that people care about privacy but nevertheless share data using geomedia could not be supported. We did not find a dichotomy between caring about data protection and usage behavior. 45% of the respondents said that they took measures to protect their privacy on the internet. Of this group, 93.5% stated that they deliberately change the privacy settings on certain apps. From the results of the quasi experiment, however, we could visualize the massive amount of data that is shared by a smartphone as soon as it is connected to WiFi, while users perform "simple" search queries or share a selfie and do not realize the hidden data-sharing processes. We agree with and emphasize Debatin's theory of a submerged part of network behavior. While the visible part (1/8 of the whole) (Debatin et al., 2009, p. 88) is seen as social networking and fun from the users' perspective (in our study the fun element is complemented by the assumed usefulness of apps), the invisible part (7/8 of the whole) (ibid.) is "constantly fed by the data that trickle down from the interactions and self-descriptions of the users in the visible part" (Debatin et al., 2009, p. 88).

According to our results, users do try to protect their privacy, but only manage to do so within what is visibly accessible to them (by changing the privacy settings, holding back certain contents, etc.). The hidden part of the data-sharing processes is non-transparent and uncontrollable. Participants said they had a vague idea of the hidden data-sharing processes but were shocked by how much our quasi-experiment revealed. This casts new light on the privacy paradox insofar as we have to consider the virtual impossibility of fully controlling data mining and marketing, aggregation, filtering and re-organization of data for purposes of targeted marketing and risk-evaluation. It seems that only the non-use of geomedia or the strict use of geomedia that resist the trend can one protect one's privacy: the AP (Associated Press) reported in August 2018 that Google saves your location history even if you have paused "location history" on your mobile device.[7] But the non-use of geomedia is not the kind of usage pattern we observed. Amongst the participants, Google Maps is the most frequently used app and the number-one tool for navigation, being used by 88.2%. 96.7% of these users utilize it for practical reasons, while 60% of the non-users don't use it because of privacy concerns. If we connect these findings with the outcome of the data collected by our research web service, we can demonstrate the enormous role that Google plays. Google can clearly be identified as one of the dominant players of the actual transformation of everyday life as Google services were the top five second-level domains to mutually exchange information. As geomedia are

[7] https://apnews.com/828aefab64d4411bac257a07c1af0ecb

"contextualizing communication" (Gryl, Jekel 2012, p. 22), regulating "social behavior and interpersonal communications" (Lapenta 2011) and changing the appropriation of space, the dominance of one big player is to be criticized as it leads to restricted diversity in favor of (Google's own) commercial benefits.

Participants in our study showed a high degree of awareness of the commercial aims behind data-sharing processes; 50% of them were even aware of the full extent of these aims (all items selected). We may argue that general awareness of problems with data collection as part of business models has increased recently due to the GDPR, which came into force on 25 May 2018, and the controversy around Cambridge Analytica. The case of Cambridge Analytica, a company that provided targeted marketing services to corporate but also political clients, and used Facebook data to influence the 2016 U.S. election, points to the political dimensions of media practices and data-sharing processes.

It could be argued that our study was self-selecting and voluntary, and that the visitors to "The Long Night of Research" were in general highly educated and more aware of the problems with data-sharing processes. This argument is supported by the fact that 46.1% of the participants had a higher school certificate, and 32.4% held a university degree. Furthermore, one could argue that only people with a certain critical approach to privacy came to our research corner. We think that these arguments are reflected in the online questionnaire, but despite our participants having a raised problem awareness, they were still not capable of controlling the hidden data-sharing processes. With this in mind, it can be stated that there is a gap between the ability to determine an appropriate flow of geodata and the actual flow of data, which is shaped by the platforms business-models and privacy policies. This gap could be seen as an expression of power imbalances between corporations and users.

Examining the geodata shared in different contexts, we discovered that contextual factors matter: the contextual usage patterns within the app categories vary significantly. Although the majority of people (52.8%) preferred not to share their location in any of the given situations, they did in some cases share a lot of information inadvertently. Depending on contextual factors, people accepted a trade-off between an intrusion into privacy and convenience. Participants were most likely to share their location with their family/partner (22.5%) and when away (20.2%). The contextual privacy approach (Nissenbaum, 2010) can be applied to geomedia and geolocation data.

GDPR may have influenced the outcome of our study as well, on the one hand by a raised general awareness of privacy as a basic human right, and on the other in a technical way. We found that although the smartphone camera was enabled to access the current location, the GPS data was not included in the Exif (which would normally be the case). Only older (non-updated) versions of software provided GPS location when the camera was location-enabled. It appears that recent software updates now restrict locational data flows.

Information about the smartphone brands, and therefore of the operating systems running and browsers used, and consequently differences in data shared, reveals the "socio-material relations" (Jansson, 2018) of smartphone usage patterns.

The relation between awareness of shared geolocation data, the usefulness of apps, the data-sharing processes that result in inadvertent sharing, and subsequent actions are complex. We hope that more research will be done to shed light on these complexities. Due to the limitations of our study, we suggest further, more generalizable, investigation of the field of (un)wittingly-shared geolocation data in the framework of economics (geomedia business models). Any recommendation for further action to advance privacy-protection mechanisms should be based on three pillars (Debatin 2011): legal regulation, ethical self-regulation (Steinmaurer & Atteneder, 2018), and privacy-enhancing technology.

We may ask whether technological design (or privacy-by-design) could foster privacy capabilities among geomedia users and whether GDPR, despite all the criticism of it, is an important step to regulate data flows. Ethical self-regulation can range from unconsidered and full adoption of geomedia to an absolute refusal to use them. Shaping the world where we live *in* geomedia requires not only technical knowledge, but also raised awareness and educational efforts in universities and schools, and for company employees.

Acknowledgements

Special thanks go to Konrad Oberwimmer for helping with statistics.

References

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

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

Altheide D. L., Snow R. P. (1979). *Media Logic*. Sage: New York.

Andrejevic M. (2005). The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. *Surveillance & Society,* vol. 2(4), pp. 479–497.

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

Bailey K. D. (1994). *Methods of Social Research* (4th ed. ed.). The Free Press: New York.

Barnes S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday,* vol. 11(9).

Barreneche C., Wilken R. (2015). Platform specificity and the politics of location data extraction. *European Journal of Cultural Studies,* vol. 18(4–5), pp. 497–513.

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

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

Christensen M., Jansson A. (2015). Complicit surveillance, interveillance, and the question of cosmopolitanism: Toward a phenomenological understanding of mediatization. *New Media & Society,* vol. 17(9), pp. 1473–1491.

Couldry N., Hepp A. (2017). The continuing lure of the mediated centre in times of deep mediatization: Media Events and its enduring legacy. *Media, Culture & Society,* vo. 40(1), pp. 114–117.

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

Debatin B., Lovejoy J. P., Horn A.-K., Hughes B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication,* vol. 15(1), pp. 83–108.

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

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

Dienlin T., Trepte S. (2014). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology,* vol. 45(3), pp. 285–297.

Estes B. (2016). Geolocation—The Risk and Benefits of a Trending Technology. *ISACA Journal,* vol. 5.

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

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

Fuchs C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication & Ethics in Society,* vol. 9(4), pp. 220–237.

Geospatial Media and Communications. (2018). GEOBUIZ. Geospatial Industry Outlook & Readiness Index. Retrieved from http://www.geobuiz.com/geobuiz-2018-report.html. 15.04.2018.

Gryl I., Jekel T. (2012). Re-centring Geoinformation in Secondary Education: Toward a Spatial Citizenship Approach. *Cartographica,* vol. 47(1), pp. 18–28.

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

Habermas J. (1962). *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft* (Vol. 1. Aufl., unveränd. Nachdr. der zuerst 1962 im Luchterhand-Verl. ersch. Ausg., erg. um ein Vorw.). Suhrkamp: Frankfurt am Main.

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

Hepp A. (2017). *Transforming Communications. Media-related Changes in Times of Deep Mediatization. Communicative Figurations – Working Paper No. 16.* ZeMKI, Zentrum für Medien-, Kommunikations- und Informationsforschung: Bremen.

Hjarvard S. (2008). The Mediatization of Society. A Theory of the Media as Agentsof Social and Cultural Change. *Nordicom Review,* vol. 29(2), pp. 105–134.

Hjarvard S. (2013). *The mediatization of culture and society* (1. publ. ed.). Routlege: London.

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

Jansson A. (2018). *Mediatization and Mobile Lives. A Critical Approach*. New York: Routledge.

Jekel T., Sanchez E., Gryl I., Juneau-Sion C., Lyon J. (Eds.). (2014). *Learning and teaching with geomedia*. Cambridge Scholars Publ.: Newcastle upon Tyne.

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

Klauser F., Widmer S. (2017). Surveillance and Control. In R. Kitchin, T. P. Lauriault, & M. W. Wilson (Eds.), *Understanding spatial media*. Sage: Los Angeles, pp. 216–224.

Krotz F. (2007). The meta-process of `mediatization' as a conceptual frame. *Global Media and Communication,* vol. 3(3), pp. 256–260.

Krotz F. (2017). Explaining the Mediatisation Approach. *Javnost – The Public,* vol. 24(2), pp. 103–118.

Lapenta F. (2011). Geomedia: on location-based media, the changing status of collective image production and the emergence of social navigation systems. *Visual Studies,* vol. 26(1), pp. 14–24.

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

Marwick A. E. (2012). The Public Domain: Surveillance in Everyday Life. *Surveillance & Society,* vol. 9(4), pp. 378–393.

Marwick A. E., boyd d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society,* vol. 16(7), pp. 1051–1067.

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

McStay A. (2017). *Privacy and the Media*. Sage: London.

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

Murdock G. (2017). Mediatisation and the Transformation of Capitalism: The Elephant in the Room. *Javnost – The Public,* vol. 24(2), pp. 119–135.

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

Nissenbaum H. (2011). A Contextual Approach to Privacy Online. *Daedalus,* vol. 140(4), pp. 32–48.

O'Neil C. (2016). Weapons of Math Destruction. *Discover,* vol. 37(8), pp. 50–55.

Rheingold H. (2002). *Smart Mobs. The Next Social Revolution*. Basic Books: New York.

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

Saker M. (2016). Foursquare and identity: Checking-in and presenting the self through location. *New Media & Society*, vol. 19 (6), pp. 934–949.

Schwartz R., Halegoua G. R. (2014). The spatial self: Location-based identity performance on social media. *New Media & Society,* vol. 17(10), pp. 1643–1660.

Steinmaurer T. (2014). Mediatized Connectivity: Historical Traits of Telephony and Theoretical Considerations about a New Dispositive of Communication. In A. Hepp, F. Krotz (Eds.), *Mediatized Worlds: Culture and Society in a Media Age*. Palgrave Macmillan: Houndmills, pp. 91–106.

Steinmaurer T., Atteneder H. (2018). Permanent Connectivity: From Modes of Restrictions to Strategies of Resistance and Questions of Digital Ethics. In T. Eberwein, M. Karmasin, F. Krotz, M. Rath (Eds.), *Responsibility and Resistance: Ethics in Mediatized Worlds*. Springer: Wiesbaden, pp. 101–117.

Thielmann T., van der Velden L., Fischer F., Vogler R. (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.

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

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

Zwick D., Dholakia N. (2001). Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right. *Electronic Markets,* vol. 11(2), pp. 116–120.

Zwick D., Dholakia N. (2004). Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing. *Journal of Macromarketing,* vol. 24(1), pp. 31–43.

Appendix 1 – Questionnaire

Dear Participants,

Thank you for supporting our research! In the context of the Austrian "Long Night of Research" at the University of Salzburg, we are conducting research on data-sharing processes. […][8]

1. Do you use sightseeing apps?
   a. Yes
      i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No
   i. For what reasons do you never use these apps?
         1. I'm not interested in them
         2. I don't know these kinds of apps
         3. For privacy reasons (I don't want to share my data)

2. Do you use apps for public transport?
a. Yes
i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No

[8] Note: original questionnaire was in German with a longer foreword!

i. For what reasons do you never use these apps?
   1. I'm not interested in them
   2. I don't know these kinds of apps
   3. For privacy reasons (I don't want to share my data)

3. Do you use weather apps?
   a. Yes
      i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No
      i. For what reasons do you never use these apps?
         1. I'm not interested in them
         2. I don't know these kind of apps
         3. For privacy reasons (I don't want to share my data)

4. Do you use Google Maps?
   a. Yes
i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No
      i. For what reasons do you never use these apps?
         1. I'm not interested in them
         2. I don't know these kinds of apps
         3. For privacy reasons (I don't want to share my data)

5. Do you use apple "Maps"?
   a. Yes
      i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No

i. For what reasons do you never use these apps?
   1. I'm not interested in them
   2. I don't know these kinds of apps
   3. For privacy reasons (I don't want to share my data)

6. Do you use social network apps?
   a. Yes
      i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No
      i. For what reasons do you never use these apps?
         1. I'm not interested in them
         2. I don't know these kinds of apps
         3. For privacy reasons (I don't want to share my data)

7. Do you use shopping apps?
   a. Yes
      i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No
      i. For what reasons do you never use these apps?
         1. I'm not interested in them
         2. I don't know these kinds of apps
         3. For privacy reasons (I don't want to share my data)

8. Do you use fitness apps?
   a. Yes
      i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No

i. For what reasons do you never use these apps?
   1. I'm not interested in them
   2. I don't know these kinds of apps
   3. For privacy reasons (I don't want to share my data)

9. Do you use dating apps?
   a. Yes
      i. For what reasons do you use these apps?
         1. Because I find them useful
         2. I use them for my work
         3. To get relevant information and to stay informed
         4. Because otherwise I'm afraid of missing something
         5. Because some/most of my friends use these apps
         6. Because some/most of my family members use these apps

   b. No
      i. For what reasons do you never use these apps?

1. I'm not interested in them
2. I don't know these kinds of apps
3. For privacy reasons (I don't want to share my data)

10. Do you use apps for delivery services (food, etc.)?
    a. Yes
       i. For what reasons do you use these apps?
          1. Because I find them useful
          2. I use them for my work
          3. To get relevant information and to stay informed
          4. Because otherwise I'm afraid of missing something
          5. Because some/most of my friends use these apps
          6. Because some/most of my family members use these apps

    b. No
       i. For what reasons do you never use these apps?
          1. I'm not interested in them
          2. I don't know these kinds of apps
          3. For privacy reasons (I don't want to share my Data)

11. Do you know how to share your location on your smartphone (positioning services)
    a. Yes
    b. No

12. In your opinion, which of the following apps uses user-data for commercial purposes?

	Yes	No
Sightseeing apps	o	o
apps for public transport	o	o
Weather apps	o	o
Google Maps	o	o

	Yes	No
Apple „Maps“	o	o
Social network apps	o	o
Shopping apps	o	o
Fitness apps	o	o
Dating apps	o	o
apps for delivery services	o	o

13. Do you usually share your location history with Google or Apple?
    a. Yes
    b. No
    c. I don't know
14. Is the camera on your smartphone enabled to access your location?
    a. Yes
    b. No
    c. I don't know
15. Are there apps on your smartphone that you always prevent from accessing your location?
    a. Yes
        i. Which ones?
    b. no
16. Which of the following apps do you allow to access to your location?

	Yes	No
Sightseeing apps	o	o
apps for public transport	o	o
Weather apps	o	o
Google Maps	o	o
apple „Maps“	o	o
Social network apps	o	o
Shopping apps	o	o
Fitness apps	o	o
Dating apps	o	o
apps for delivery services	o	o

17. Please rate the following statements (Scale: 1= totally agree; 5= totally disagree)
    a. It bothers me that my app-usage behaviour is traceable
    b. I don't care much about the usage of my data online
    c. It bothers me that my user-data is shared with "third parties"
    d. In general, I am fairly concerned about data protection and privacy on the internet
    e. I don't feel capable of protecting my data online
    f. I don't have time to be bothered about the topic of privacy
    g. I don't have the time to deal with that topic

18. In which of the following situations do you share your location (multiple choice)?
    a. Normally, I share my location with my family/my partner so that they know exactly who is where.
    b. I usually share my location with friends (e.g. to arrange an exact meeting place)

c. When sharing pictures, I usually share my location consciously (GPS)
d. Within my professional network, I have to share my current location
e. I share my location with my family/my friends/my partner when I'm away
f. I share my current routes and performance when doing sports
g. In none of the given situations

19. Did you participate in the experiment at the "Long Night of Science 2018"?
    a. Yes
        i. Before the experiment, were you aware of sharing data with (hidden) domains when doing a simple search query?
            1. Yes
            2. No

b. No

20. Do you actively protect your personal data on the internet?
    a. Yes
        i. Which of the following measures do you take?
            1. I consciously change the privacy settings of certain apps
            2. I refuse to use certain apps/platforms for privacy reasons
            3. I use an encrypted E-Mail service
            4. I use a search engine that doesn't track my search behaviour
            5. Location services are generally disabled on my smartphone
    b. No

21. Finally, please provide us with some information about yourself:
22. How old are you? _____
23. What is your highest level of successfully completed education?
24. Are you male/female?
25. Could we contact you for a further in-depth qualitative interview?

a. Yes
    i. Please leave your contact information:
b. No

Thank you for participating!

Appendix 2 – Number of hits for second-level domains (hits per domain)

713 google.com.
367 apple.com.
311 googleapis.com.
217 gstatic.com.
138 google.at.
123 googleusercontent.com.
108 icloud.com.
98 facebook.com.
86 ac.at.
74 doubleclick.net.
62 whatsapp.net.
48 apple-dns.net.
44 ampproject.org.
43 googleadservices.com.
36 samsung.com.
35 orf.at.

28 akamaiedge.net.
27 google-analytics.com.
26 android.com.
25 crashlytics.com.
22 zeit.de.
22 googletagmanager.com.
21 oewabox.at.
21 instagram.com.
21 glpals.com.
21 fbcdn.net.
20 samqaicongen.com.
19 youtube.com.
16 yahoo.com.
16 googlesyndication.com.
16 cloudfront.net.
15 amazonaws.com.
12 twitter.com.
12 samsungapps.com.
12 bing.com.
12 adnxs.com.
11 digicert.com.
11 avast.com.
11 akadns.net.
10 yimg.com.
10 samsungcloud.com.
10 ntp.org.
10 meetrics.net.
10 letsencrypt.org.
10 gvt1.com.
10 google.de.
9 ksmobile.net.
9 hicloud.com.
9 googlezip.net.
9 gmx.net.
9 game-mode.net.
9 amazonvideo.com.
8 skype.com.
8 microsoft.com.
8 ligatus.com.
8 googletagservices.com.
8 gmail.com.
8 cmcm.com.
7 spotify.com.
7 ksmobile.com.
7 fb.com.
7 facebook.net.
7 demdex.net.
7 cdninstagram.com.
7 appsflyer.com.
7 adjust.com.
7 1und1.de.
6 weather.com.
6 twimg.com.
6 snapchat.com.
6 secb2b.com.
6 samsungpositioning.com.
6 outlook.com.
6 mozilla.com.
6 moatads.com.
6 ioam.de.
6 identrust.com.
6 gvt3.com.
6 gvt2.com.
6 app-measurement.com.
6 applovin.com.
6 amazon.com.
6 accuweather.com.
6 aaplimg.com.
5 zeitverlag.de.
5 wp.com.
5 ui-portal.de.
5 intercom.io.
5 ggpht.com.
5 gebrauchtwagen.at.
5 gdatasecurity.de.
5 cloudflare.com.
5 adition.com.
5 adform.net.
5 a1.net.
5 3gppnetwork.org.
4 ytimg.com.
4 tclclouds.com.
4 spaghettiundco.com.
4 solarmovie.ph.
4 scorecardresearch.com.
4 rfihub.com.
4 qualtrics.com.
4 pinterest.com.
4 outbrain.com.
4 opera.com.
4 msn.com.
4 mozilla.net.
4 mixpanel.com.
4 lijit.com.
4 lastella-salzburg.at.
4 krone.at.

4 exactag.com.
4 eset.com.
4 apester.com.
4 addthis.com.
3 zeropc.com.
3 whatsapp.com.
3 uicdn.com.
3 t.co.
3 tapad.com.
3 ssl-images-amazon.com.
3 sfx.ms.
3 samsungosp.com.
3 rubiconproject.com.
3 peel-prod.com.
3 netdoktor.de.
3 mxcdn.net.
3 mopub.com.
3 mathtag.com.
3 iocnt.net.
3 htcsense.com.
3 htc.com.
3 duckduckgo.com.
3 dsp.io.
3 disqus.com.
3 diepresse.com.
3 combotag.com.
3 casalemedia.com.
3 bidswitch.net.
3 avcdn.net.
3 amazon-adsystem.com.
3 agkn.com.
3 advertising.com.
3 adsafeprotected.com.
3 adkmob.com.
3 accountkit.com.
2 zendesk.com.
2 zeitakademie.de.
2 zdbb.net.
2 xing.com.
2 w.org.
2 wordpress.com.
2 woman.at.
2 willhaben.at.
2 web.de.
2 vi-serve.com.
2 vimeo.com.
2 vimeocdn.com.
2 viber.com.
2 upalytics.com.
2 uimserv.net.
2 typekit.net.
2 twitch.tv.
2 twiago.com.
2 tunein.com.
2 tumblr.com.
2 theadex.com.
2 telering.at.
2 symcd.com.
2 styria-digital.com.
2 studo.co.
2 stickyadstv.com.
2 staticfiles.at.
2 scrm.com.
2 sascdn.com.
2 samsungdm.com.
2 samsung.de.
2 salzburg24.at.
2 pushwoosh.com.
2 primevideo.com.
2 powerlinks.com.
2 plista.com.
2 pinimg.com.
2 paypal.com.
2 ospserver.net.
2 optmstr.com.
2 openx.net.
2 onelink.me.
2 omtrdc.net.
2 netmng.com.
2 netflix.com.
2 myqnapcloud.com.
2 musical.ly.
2 mozilla.org.
2 mgccw.com.
2 mcdonalds.at.
2 maps.me.
2 mail.ru.
2 linkedin.com.
2 ligadx.com.
2 launchdarkly.com.
2 krxd.net.
2 isnssdk.com.
2 ip-api.com.
2 interestingprizesforyou.stream.
2 icloud-content.com.
2 hshh.org.

2 h-bid.com.
2 gwallet.com.
2 google.it.
2 fqtag.com.
2 flipboard.com.
2 exelator.com.
2 ebay.com.
2 disquscdn.com.
2 ctnsnet.com.
2 crwdcntrl.net.
2 criteo.com.
2 co.uk.
2 chip.de.
2 blogspot.com.
2 beusable.net.
2 avaaz.org.
2 app.link.
2 aniview.com.
2 amazon.de.
2 akamai.net.
2 agoda.com.
2 adworx.at.
2 adsrvr.org.
2 adobe.com.
2 2mdn.net.
1 zooverresources.com.
1 zoover.nl.
1 ziffdavis.com.
1 zhiliaoapp.com.
1 ze.tt.
1 zeit-verlagsgruppe.de.
1 zeit-verlag.de.
1 zeitabo.de.
1 yieldmo.com.
1 yieldlab.net.
1 yesss.at.
1 yahooapis.com.
1 yabidos.com.
1 wps.com.
1 wix.com.
1 wikipedia.org.
1 whispersystems.org.
1 weltkunst.de.
1 weborama.fr.
1 wbtrk.net.
1 was-tuat-si.at.
1 w55c.net.
1 vtracy.de.
1 vk.com.
1 visualdna.com.
1 veruta.com.
1 userreport.com.
1 ursulinen-salzburg.at.
1 unsplash.com.
1 uni-salzburg.at.
1 umfrageonline.com.
1 uefa.com.
1 ubimet.com.
1 twyn.com.
1 turn.com.
1 ttvnw.net.
1 trustx.org.
1 truste.com.
1 trustarc.com.
1 tiqcdn.com.
1 tifbs.net.
1 thunderhead.com.
1 styria-publishing.com.
1 statcounter.com.
1 spotxchange.com.
1 spektrum.de.
1 speedtest.net.
1 spar.at.
1 solarmovie.so.
1 smartstream.tv.
1 sitescout.com.
1 siteimprove.com.
1 siteimproveanalytics.com.
1 simpli.fi.
1 sharethrough.com.
1 serving-sys.com.
1 semasio.net.
1 seadform.net.
1 salzburgresearch.at.
1 salzburg-altstadt.at.
1 rvs.at.
1 rutarget.ru.
1 runtastic.com.
1 roteskreuz.at.
1 rlcdn.com.
1 revolutionevent.com.
1 realmadrid.es.
1 rayjump.com.
1 quatscha.at.
1 quantcount.com.
1 qq.com.

1 pubmatic.com.
1 polyfill.io.
1 pizzeria-daciro.at.
1 pizzamann.at.
1 pesthaus.at.
1 osteria-cavalli.at.
1 opera.software.
1 opera-api.com.
1 onesignal.com.
1 onaudience.com.
1 office365.com.
1 oebb.at.
1 obvsg.at.
1 ntracecloud.com.
1 nr-data.net.
1 nmapps.de.
1 nict.jp.
1 nexage.com.
1 nexac.com.
1 newrelic.com.
1 ndimg.de.
1 narando.com.
1 my-samsung.com.
1 myfonts.net.
1 mstrlytcs.com.
1 mobpalm.com.
1 mobimagic.com.
1 mobile.de.
1 ml314.com.
1 mjam.net.
1 mindtake.com.
1 mindbreeze.com.
1 microsoftonline-p.com.
1 microsoftonline.com.
1 mein-fussabdruck.at.
1 mediatek.com.
1 media.net.
1 media-amazon.com.
1 media6degrees.com.
1 me.com.
1 mcafee.com.
1 lqm.io.
1 lqmcdn.com.
1 liverpoolfc.tv.
1 live.net.
1 linguatec.org.
1 ligaportal.at.
1 lidlplus.com.
1 liadm.com.
1 leanplum.com.
1 langenachtderforschung.at.
1 ksosoft.com.
1 kleinezeitung.at.
1 kingsoft-office-service.com.
1 kingsoft.com.
1 keytiles.com.
1 juliasellmann.com.
1 jsdelivr.net.
1 jquery.com.
1 jpush.cn.
1 ixiaa.com.
1 isappcloud.com.
1 irquest.com.
1 iroither.at.
1 iqm.de.
1 iqcontentplatform.de.
1 indivsurvey.de.
1 imrworldwide.com.
1 immowelt.de.
1 ib-ibi.com.
1 hs-data.com.
1 hotmail.com.
1 hothardware.com.
1 hotelmediaservice.com.
1 hello-october.com.
1 haui.eu.
1 harrycloudfoot.com.
1 gumgum.com.
1 gssprt.jp.
1 grm-pro.com.
1 gravatar.com.
1 googlevideo.com.
1 googlemail.com.
1 google.es.
1 goo.gl.
1 go-mpulse.net.
1 goetz-motorsport.de.
1 glotgrx.com.
1 getpebble.com.
1 gdatasoftware.com.
1 g.cn.
1 fyber.com.
1 flickr.com.
1 finanzen.net.
1 fcbayern.com.
1 faistenau-online.at.

1 eyereturn.com.
1 eyeota.net.
1 eyeem.com.
1 extremereach.io.
1 exlibrisgroup.com.
1 eurowings.com.
1 etsy.com.
1 eslgaming.com.
1 enuvo.ch.
1 entrust.net.
1 emetriq.de.
1 electriclove.at.
1 elba.at.
1 eingutertag.org.
1 e-fellows.net.
1 edgekey.net.
1 ebay-us.com.
1 ebayimg.com.
1 ebay.de.
1 dyntrk.com.
1 duapps.com.
1 dropbox.com.
1 drei.at.
1 dotomi.com.
1 direct.ly.
1 digitru.st.
1 derstandard.at.
1 dept1.de.
1 de.com.
1 dbankcdn.com.
1 datenschutz-grundverordnung.eu.
1 cxense.com.
1 cryptocompare.com.
1 classistatic.de.
1 calista.at.
1 btc-echo.de.
1 brandeins.de.
1 brandcrumb.com.
1 bnc.lt.
1 bluemailapp.com.
1 bluekai.com.
1 bitstrips.com.
1 bitmoji.com.
1 bidtheatre.com.
1 bidr.io.
1 bergbahnen-werfenweng.com.
1 bellevue-ferienhaus.de.
1 batmobi.net.
1 basebanner.com.
1 avg.com.
1 avazutracking.net.
1 avazunativeads.com.
1 autohaus-traunreut.de.
1 atdmt.com.
1 asroma.it.
1 ask.com.
1 asideas.de.
1 appspot.com.
1 appboy.com.
1 apa.at.
1 anrdoezrs.net.
1 anime-mura.de.
1 angsrvr.com.
1 amelialiana.com.
1 allunite.com.
1 alipay.com.
1 akstat.io.
1 akamaihd.net.
1 airbnb.com.
1 adziff.com.
1 adsymptotic.com.
1 adservice.at.
1 adscale.de.
1 adsafety.net.
1 adrtx.net.
1 adriver.ru.
1 adobedtm.com.
1 adingo.jp.
1 adhigh.net.
1 addthisedge.com.
1 active-agent.com.
1 accu-weather.com.
1 a1community.net.
1 3lift.com.
1 360yield.com.
1 360safe.com.
1 1rx.io.

Appendix 3 – Top 90 list of fully qualified domain names (hits per domain)

359 www.google.com.
83 universum.sbg.ac.at.
82 connectivitycheck.gstatic.com.
78 www.google.at.
56 android.clients.google.com.
53 play.googleapis.com.
50 www.googleapis.com.
47 clients4.google.com.
46 mtalk.google.com.
43 clients3.google.com.
43 www.googleadservices.com.
41 android.googleapis.com.
41 lh5.googleusercontent.com.
39 www.gstatic.com.
35 apple.com.
35 clients1.google.com.
34 adservice.google.at.
34 cdn.ampproject.org.
34 lh3.googleusercontent.com.
34 www.apple.com.
32 captive.apple.com.
32 graph.facebook.com.
31 googleads.g.doubleclick.net.
29 www.icloud.com.
28 g.whatsapp.net.
27 api-glb-fra.smoot.apple.com.
27 mmg-fna.whatsapp.net.
25 connectivitycheck.android.com.
23 accounts.google.com.
23 lh4.googleusercontent.com.
22 adservice.google.com.
22 configuration.apple.com.
22 encrypted-tbn0.gstatic.com.
22 lh6.googleusercontent.com.
22 www.googletagmanager.com.
21 maps.gstatic.com.
20 gs-loc.apple.com.
20 id.google.at.
20 maps.googleapis.com.
19 ad.doubleclick.net.
18 mesu.apple.com.
18 safebrowsing.googleapis.com.
18 settings.crashlytics.com.
18 translate.googleapis.com.
17 www.facebook.com.
16 fonts.gstatic.com.
16 mobilemaps-pa.googleapis.com.
16 www.google-analytics.com.
15 fonts.googleapis.com.
15 gateway.icloud.com.
14 clientservices.googleapis.com.
14 mqtt-mini.facebook.com.
12 cl2.apple.com.
12 e6858.dsce9.akamaiedge.net.
12 init.itunes.apple.com.
12 www.youtube.com.
11 gsp64-ssl.ls.apple.com.
11 ocsp.digicert.com.
11 ssl.google-analytics.com.
11 supl.google.com.
10 chromecontentsuggestions-pa.googleapis.com.
10 edge-mqtt.facebook.com.
10 ocsp.int-x3.letsencrypt.org.
10 s.yimg.com.
10 www.bing.com.
9 gateway.fe.apple-dns.net.
9 gllto.glpals.com.
9 google.com.
9 graph.instagram.com.
9 guzzoni.apple.com.
9 mtalk4.google.com.
9 promo.webpayments.closeby.internet.apps.samsung.com.
9 time-ios.apple.com.
9 update.googleapis.com.
9 vas.samsungapps.com.
8 api.samsungcloud.com.
8 datasaver.googleapis.com.
8 geomobileservices-pa.googleapis.com.
8 imap.gmail.com.
8 mobile.pipe.aria.microsoft.com.
8 pagead2.googlesyndication.com.
8 service.game-mode.net.
8 setup.icloud.com.
8 ssl.gstatic.com.
8 stats.g.doubleclick.net.
8 www.googletagservices.com.
7 2.android.pool.ntp.org.
7 app.adjust.com.
7 at.search.yahoo.com.
7 connect.facebook.net.