Article

new media & society
2021, Vol. 23(6) 1443–1464
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1461444820905045
journals.sagepub.com/home/nms
SAGE

Linking loose ends: An interdisciplinary privacy and communication model

Katharina Bräunlich
University of Koblenz-Landau, Germany

Tobias Dienlin
University of Hohenheim, Germany

Johannes Eichenhofer
Bielefeld University, Germany

Paula Helm
Goethe University Frankfurt, Germany

Sabine Trepte
University of Hohenheim, Germany

Rüdiger Grimm
University of Koblenz-Landau, Germany

Sandra Seubert
Goethe University Frankfurt, Germany

Christoph Gusy
Bielefeld University, Germany

Corresponding author:
Katharina Bräunlich, University of Koblenz-Landau, Universitätsstrasse 1, 56070 Koblenz, Germany.
Email: braeunlich@uni-koblenz.de

Abstract

In the recent decades, privacy scholarship has made significant progress. Most of it was achieved in monodisciplinary works. However, privacy has a deeply interdisciplinary nature. Most importantly, societies as well as individuals experience privacy as being influenced by legal, technical, and social norms and structures. In this article, we hence attempt to connect insights of different academic disciplines into a joint model, an Interdisciplinary Privacy and Communication Model. The model differentiates four different elements: communication context, protection needs, threat and risk analysis, as well as protection enforcement. On the one hand, with this model, we aim to describe how privacy unfolds. On the other hand, the model also prescribes how privacy can be furnished and regulated. As such, the model contributes to a general understanding of privacy as a theoretical guide and offers a practical basis to address new challenges of the digital age.

Keywords

Communication, interdisciplinary, legal, model, privacy, social, technical

Introduction

Privacy is fundamentally important—both for individuals and for societies. Privacy fosters psychological well-being and promotes individual autonomy (Petronio, 2002). Moreover, privacy serves the society as a whole, for example, by generating and preserving areas of diversity and pluralism, which every democracy depends on (Bennet, 2015). Each of these functions has been challenged in the age of modern information and communication technology (ICT): zones of autonomy and intimacy seem to disappear, (authoritarian) regimes make extensive use of Internet surveillance measures and the line between private and public information seems to blur. Due to these developments, privacy has experienced a fundamental transformation and has become one of the most relevant topics of the current millennium. However, it has often been stated that privacy is a contested and multidimensional concept, full of puzzles and inherent paradoxes (Nissenbaum, 2009). Although we agree, fortunately during the last decades, various valuable insights have been produced, which have increased our understanding significantly. This includes the perception and conceptualization of privacy (Cohen, 2012), its instrumental value (Rössler, 2001), its legal boundaries (Solove, 2008), its digital realization (Cavoukian, 2009), its individual management (Petronio, 2002), and its societal manifestation (Nissenbaum, 2009). In full acknowledgment of these progresses, we nonetheless see two research gaps, which we seek to address in this article.

It has become increasingly apparent that privacy is deeply interdisciplinary, because it is enacted through legal, technical, and social norms and in respective structures. In this article, we therefore continue and extend prior interdisciplinary privacy research (e.g. Nissenbaum, 2009) by connecting several of the above-mentioned insights into an overarching Interdisciplinary Privacy and Communication Model (IPCM). Specifically, we combine the four perspectives of communication science, social and political science, computer science, and legal sciences. While modeling this interdisciplinary picture on privacy, we take into account that privacy is deeply influenced by the specific cultural and political standpoints from which we are drawing it (Haraway, 1988).

The IPCM contributes to bridge the gap between research and practice, because it can be operationalized in at least two concrete ways: First, the IPCM provides interfaces to well-established processes from IT security (ISO/IEC 27005:2018, 2018) as well as from requirements engineering (IEEE 29148-2018, 2018). While this adoption and the precise method-based embedding of the IPCM into the whole software development life cycle (SDLC) (IEEE 12207-2017, 2017) is future work, the IPCM can be seen as an important step toward privacy by design. Second, the IPCM's components intentionally show parallels to well-established evaluation and certification standards such as Common Criteria (ISO/IEC 15408:2009, 2009) envisioning the future evaluation and certification of IT products or systems with respect to their socio-political, psychological, and legal consequences and its accordance with democratic constitutions and fundamental rights.

This article is structured as follows: First, each discipline discusses privacy as a theoretical concept, presenting relevant insights that we later include in our interdisciplinary model. Thereafter, we present our general understanding of communication. We then synthesize these monodisciplinary insights, explaining each of its components and their mutual relationship. By applying our model to a specific use case, we then elucidate the privacy-relevant characteristics of digital communication. We conclude with a general discussion and critical reflection of our work.

Privacy in the digital age—established concepts and new perspectives

In all disciplines, the term *privacy* or *private life* refers to a specific form of social life, which can be distinguished from *public life*. Private life can occur in private rooms (*local privacy*), in the communication of private information (*informational privacy*), and in taking private decisions (*decisional privacy*) (Rössler, 2001). The following two concepts feature in almost all definitions and understandings of privacy (Masur, 2018): *limitation of access*[1] and *control of access.*[2] Privacy as limitation of access builds on Warren and Brandeis (1890), who understood privacy as "right to be let alone" (p. 195). Privacy as control of access considers privacy as "an individual's right to control information about them and decide when, how, and to what extent information is communicated to others" (Westin, 1967: 7). In addition to these meta-disciplinary understandings of privacy, there also exist more disciplinary-specific ones, which we present in what follows. Please note that boundaries are not clear-cut and that several understandings overlap.

Communication science

Communication science analyzes privacy by focusing on the individual (Altman, 1975). This has several implications. For example, it can lead to the distinction of an *objective privacy context* and a *subjective privacy perception* (Dienlin, 2014). The objective privacy context captures the extent to which people are accessible and in control of this accessibility; it can be measured by determining, for example, audience size and physical proximity. The subjective privacy perception captures how private people feel and what they need (Westin, 1967); it can be measured by means of conventional self-reports. Both levels often differ. Especially in various online contexts, the subjective privacy is often high, whereas the objective privacy is actually low (Trepte and Reinecke, 2011).

People constantly engage in so-called privacy regulation behaviors. There exist two major forms: *preventive privacy regulation* (e.g. sending someone an encrypted e-mail) or *corrective privacy regulation* (e.g. deleting an e-mail) (Masur, 2018: 61). A primary mechanism to regulate privacy is self-disclosure, which exhibits an inverse relationship with privacy (Westin, 1967): When people feel sufficiently private, they are willing to self-disclose; at the same time, when people self-disclose they also reduce their privacy. As a result, people set-up both implicit and explicit boundary rules, which govern what information to disclose and what to withhold (Petronio, 2002). When these rules have either not yet been established or have been violated, information can leak to unwanted audiences, causing so-called boundary turbulences (Petronio, 2002)—which are especially likely to take place on social media, where several contexts collapse into a single one (boyd, 2014).

A current focus is to understand if, when, and why people self-disclose. For example, building on the privacy calculus model (Laufer and Wolfe, 1977), people are more likely to disclose information when they expect benefits such as social support, while they are less likely to disclose when they experience costs such as privacy concerns (Dienlin and Metzger, 2016). At the same time, privacy regulations can also be influenced by more implicit heuristic appraisal processes (Sundar et al., 2013). Moreover, self-disclosure can be increased also by means of specific (e.g. social) context cues on social networking sites (Trepte, 2020; see also the "Computer science" section). As a result, privacy is increasingly understood as being socially determined, that it is *interdependent* (Marwick and boyd, 2014; see also the "Social and political science" section); also, the role of "control" and how it is replaced by trust in realizing interdependent privacy has newly been defined (Trepte, 2020; see also the "Legal sciences" section).

Social and political science

Recent transformations in our communicative infrastructures have pointed political scientists and sociologists toward investigating the *interdependent relationship* between privacy and communication. This new focus has led to a reconceptualization of privacy. Instead of studying privacy primarily with regard to the individual, as is characteristic for communication science (see the "Communication science" section), social scientists shift the focus on the social and political dimensions of privacy. Through this, the idea of relating privacy to boundaries and boundary rules has transferred to an understanding of privacy as the *intersubjective negotiation of boundaries* (Cohen, 2012). This intersubjective approach is widely appreciated for being capable of reaching beyond an understanding of privacy as individual control and for highlighting the interdependent meaning of privacy as a common good (Regan, 2002), whose enactment and protection has to be treated as a democratic challenge (Helm and Seubert, 2020).

Approaching privacy as a social practice situated in a digital age has also provoked new perspectives on the use and value of privacy. Instead of concentrating primarily on privacy's function as a means to withdraw from society, practices of privacy are being evaluated more generally and at the same time more specifically in regard to the integrity of particular contexts (Nissenbaum, 2009). These contexts not only include obvious ones like those related to family life and intimacy but also professional, artistic, medical, and even political ones. Hence, the idea of a dichotomy between the private and the public is being deconstructed in light of a more praxis-oriented understanding focusing on the socially productive interplay between the two (Warner, 2002).

Another aspect refers to the relevance of privacy for the cultivation of a democratic public (Becker and Seubert, 2016). In light of the precarity of privacy (see the "Computer science" section), some of the most relevant political struggles within liberal democratic societies focused on this matter (Bennet, 2015). Here, it is not primarily the traditional legal claim of individuals who want to be left alone (Warren and Brandeis, 1890; see also the "Legal sciences" section) but rather the (political) claim of (political) collectives, who struggle for communicative autonomy by claiming new rights, like for instance, the right to anonymous speech online.[3] Privacy, here, is being enacted as a condition for political activism, rather than as a counterpart to the political, as it has been suggested throughout the liberal tradition (Isin and Ruppert-Schulze, 2015).

Computer science

Computer science mainly follows a construction-oriented, engineering research paradigm and thus tends to focus on the (practical) realization of privacy rather than its (theoretical) conceptualization. Often, privacy and data protection are used synonymously.[4] Based on that (mis-)understanding (see the "Social and political science" section), the focus is on the realization of data protection, primarily by implementing the data protection principles such as data minimization, purpose limitation, accuracy, fairness, transparency, or accountability.

Another line of research addresses the *realization* of privacy in terms of security requirements such as confidentiality and/or pseudonymity/anonymity (Pfitzmann and Köhntopp, 2001). They can be supported by security mechanisms, which includes encryption (Schneier, 1996), access control (Ruj et al., 2012), identity management (Hansen et al., 2008) and is realized by privacy-enhancing tools such as anonymizing remailer (Danezis et al., 2003), anonymizing browsers such as Tor,[5] or cryptocurrencies such as Bitcoin (Androulaki et al., 2013).

In 2009, the *privacy by design* framework was published (Cavoukian, 2009) and adopted as a new line of research. The basic idea of privacy by design is that privacy should not be considered as a retroactive add-on but that it should be taken into account through the whole IT lifecycle: In the early phases of technical development, privacy-enhancing principles must be incorporated into system's design. Later, in the operation phase, organizational rules and related technical parameters must not only serve efficiency, but also privacy.

On the analytic side of research, computer science discloses weaknesses of existing technology that can be exploited to violate privacy and threaten democratic systems (see the "Social and political science" section). With respect to this, there is especially in the field of IT security a range of well-established tools and methods available, for example, ISO/IEC 27000:2018 (2018) or ISO/IEC 15408:2009 (2009). They all have in common that they correlate requirements, threats, and measures. *Requirements* represent the desirable system properties. *Threats* exploit vulnerabilities of (IT) systems and violate these requirements and which need to be defended by effective security measures (Grimm et al., 2014).

Legal sciences

Law has a strong affinity toward the concept of privacy. Many of the most influential privacy theorists, in fact, were legal scientists (for an overview, see Solove, 2008). That applies to Warren and Brandeis (1890) and their "right to be left alone" or to Westin (1967) and his concept of privacy as an individual right to *limit* and *control the access to personal information*, which could be extended to personal *spaces* or *decisions* (Gusy et al., 2016: 385). Legal science is able to connect the abstract level of privacy norms with the concrete level of individual and social privacy negotiation (see the "Social and political science" section). Legal norms form an integral part of any communication context and might influence the individual communication behavior (see the "Communication science" section). They can grant the individual *subjective rights* to communicate and/or limit access to personal information toward others. Moreover, they can oblige the state or private parties to respect the individuals' privacy through the means of *objective law*, such as criminal or data protection law.

The extent to which privacy is being regulated through objective law differs from country to country (for an overview, see Bygrave, 2014). In general, lawmakers tend to distinguish between societal contexts (see the "Social and political science" section): some contexts require sharing sensitive information, like in health care or in the relation between lawyer and client. Here, specific legal safeguards to confidentiality are being specified in legal orders. The communication of less sensitive information is less regulated. The (data protection) law leaves it up to the individual to give her or his consent to the use of that information. Recently, the idea of notice and consent has been harshly criticized in privacy law as well as in political science (Helm and Seubert, 2020), due to the little amount of control it gives the users (Hartzog and Richards, 2016), especially with regard to the Internet. Hence, many legal scientists debate about the need for a further regulation (Gusy et al., 2016: 385) or self-regulation (Fernback and Papacharissi, 2007) or for replacing the control- through a trust-paradigm (Eichenhofer, 2016; Hartzog and Richards, 2016).

Communication in the digital age

The advent of smartphones and the popularity of social networking sites such as Twitter, Facebook, or Instagram (Chugh, 2012: Chapter 3) demonstrate that privacy is interweaved closely with communication. Today, much of our communicative infrastructures rely on a multitude of ICTs (Van Den berg et al., 2012), which allow third parties and intermediaries to craft user profiles that threaten privacy and the individual and democratic values it is meant to protect (Fernback and Papacharissi, 2007). But what exactly is communication? In the humanities and the social sciences, we can identify two main traditions of conceptualizing communication: On the one hand, there is *action theory*. Here, communication is understood to be a specific form of interaction between two or

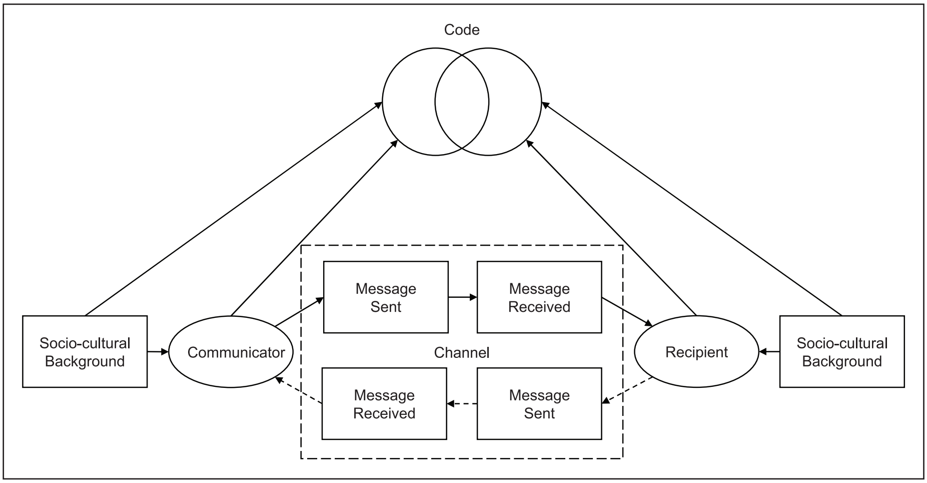

Figure 1. Communicator-recipient-model, based on Prakke (1968).

more persons who strive toward mutual understanding and consensus (Habermas, 1995). In this understanding, the influence of implicit knowledge attributed to specific life-worlds is being reflected as part of specific contexts and conditions which determine communication (Habermas, 1995: Chapter 5). On the other hand, there is *system theory*. Here, communication is understood as the convergence of information, message, and understanding and as a specific form of operation through which systems are being produced and sustained (Luhman, 1988). In both traditions, communication is conceptualized as fundamental for democratic systems.

Today, democratic systems are crucially influenced by the design and use of new ICTs (Bozdag and Van den Hoven, 2015). Therefore, we need an understanding of communication that allows us to take into account these specifics. Communication is described in the following by means of a traditional *communicator-recipient-model* (CRM) (Merten, 1977; Prakke, 1968), which is the premise of our privacy model (see the "Interdisciplinary privacy and communication model" section). The CRM in its original version, however, does not allow to fully explicate modern day communication, which is why we both extend and specify several of its tenets (see below).

According to CRM, communication is defined as the *exchange of messages between a communicator and a recipient* (see Figure 1). The messages consist of data. In the digital context, *data* is defined as any possible sequence of characters—for example, letters, numbers, or symbols. Using code, these data can then be interpreted in order to derive meaningful *information* (e.g. by adding context, abduction, deduction, or statistics) (Grimm and Delfmann, 2017).

A message is sent by the communicator to a recipient using a *channel*. The channel describes the application and medium. Examples for *applications* are e-mail, chat, or the World Wide Web. Depending on the application, the sender has to translate his or her communication into a *message*. Thus, a message can be a written text, a click on a button, or an audio or video file. Next, the message is transmitted via a *medium*, which in our model is the Internet. Due to the layered logic of the Internet (IETF RFC 1122, 1989a; IETF RFC 1123, 1989b), digital communication does not solely consist of the message itself; it also includes metadata, which depend on the application and the underlying protocol of the Internet technology. The message is then received and interpreted by the recipient.

Originally, communicator and recipient were thought to be human beings. But this model is also applicable to *person-computer-communication* (e.g. a person performing a search query or an online shop triggering a costumer with personalized newsletters) and *computer-computer-communication* (e.g. automated synchronization events between smartphones and cloud storage services). Thereby, any *smart* electronic device is regarded as a computer, including PCs, smartphones, watches, or even TVs and fridges. Here, again a broad concept of communication allows to include these cases, which is essential to fully investigating privacy-related issues in the digital age.

Furthermore, communication can be active or passive. *Active* disclosures are personal publishing on a social network site or giving permission for publication of a photo on a friend's Instagram account. In contrast, *passive* disclosure usually happens by acceptance, for example, by using a search engine.

Similarly, communication can be *intended*, for example, by speaking words out loud, or *unintended*, for example, by blushing. Also, online communication can be intended, for example, by texting or writing an e-mail, or unintended, for example, when a flashlight app on a smartphone is transmitting location data. In digital communication, both cases are privacy-relevant because any transmission of data, intended or not, can and probably will be used for information extraction.

Exchanges can be reciprocal, but do not have to be. For example, a user who performs an online search is a communicator when sending a search query to the search engine and a recipient when receiving the search results, and vice versa.

Finally, the CRM implicitly takes into account that communication takes place in a defined social environment and is thus embedded in a sociocultural system fraught by governmental logics and norms. In our case, these norms and logics are predominantly characterized by neo-liberal democratic systems. These systems are currently widening the scope of economic influence with a new data industry that is increasingly shaping communicative infrastructures online and hence communication in general. In critical media studies, for instance, this development has been criticized as an economic colonialization of the lifeworld (Betancourt, 2016).

The CRM, alongside our modifications and specifications, thereby serves as a basic framework to understand general communication processes. However, the CRM by itself does not allow to capture all the intricate privacy-related processes taking place in an increasingly digitized world (Wessels, 2012). To this end, we also need to explicitly account for psychological dispositions, technical processes, legal frameworks, and sociopolitical ramifications.

The interdisciplinary privacy and communication model

In what follows, we combine the aforementioned aspects into one overarching framework. In order to handle complexity, modeling is a well-established method in computer

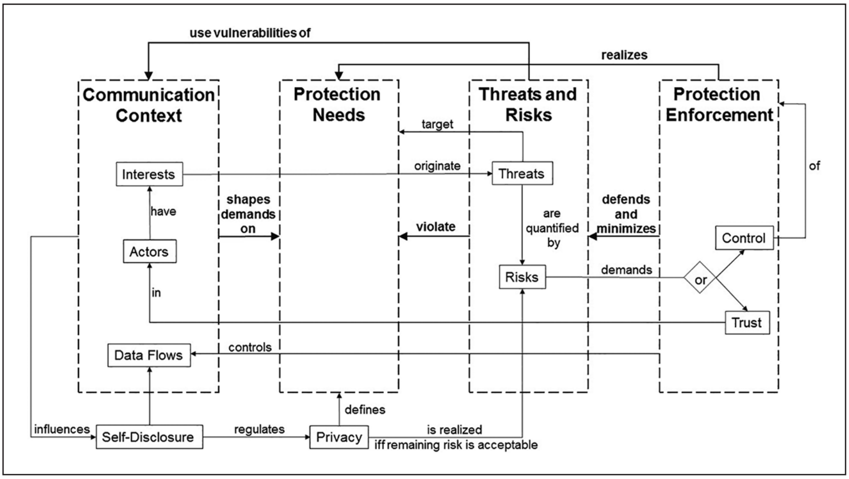

Figure 2. Relationship of the components of the IPCM.

and communication science.[6] Thereby, a *model* is defined as a contingent image of reality that emphasizes aspects relevant to a particular purpose and that abstracts from all others (Grimm and Delfmann, 2017).

The IPCM is based on four mutually related pillars—the communication context, protection needs, threat and risk analysis, and protection enforcement. The willingness to share information depends on the *communication context*. The communication context and its inherent social norms and expectations define the *protection needs*, which represent psychological, social, political, legal, and technological requirements that are important to preserve the user's privacy. These protection needs are challenged by *threats*, which exploit vulnerabilities of the communication context such as poorly implemented encryption algorithms. Threats are quantified by their *risk*. In order to defend these threats and to minimize their risk effective *protection enforcement* has to be implemented. While the first pillar is directly derived from the entanglement of privacy and communication, the last three pillars are well-established categorizations in IT security analysis (Grimm et al., 2014).

The IPCM contributes to a better conceptualization of privacy by explicating its concepts, attributes, and their ontological relationship as illustrated in Figure 2. Furthermore, several components provide interfaces to well-established processes from IT security (ISO/IEC 27005:2018, 2018), which facilitates the future operationalization of the IPCM.

Communication context

As stated above, privacy closely relates to communication and self-disclosure. The willingness of an individual to share information takes place within and is influenced by the *communication context.* To best understand human behavior, we need to analyze its context, the perceptions thereof, and how both dynamically interact (Trepte, 2020).

One major determinant of the context are the *actors* who are involved in the communication. Actors can be human beings, institutions, or computers. When describing contexts, we refer only to directly and legitimately involved actors. Later, as part of the threat and risk analysis, possible attackers have to be identified, including, for example, criminals, commercial data miners, or government agencies such as law enforcement or intelligence agencies. All involved actors are classified by their *domain*. Possible domains are public space, working environment, friends and family, services, homes, and third parties. It has to be noted that the domains are not necessarily disjoint. For example, it is possible that a communication partner is a friend and a colleague at the same time.

Whether or not privacy is respected depends on the context and the norms that restrict, allow, or determine the way information flows—both within the context and between different contexts (for the concept of contextual integrity, but with a different understanding of context, see Nissenbaum, 2009). Therefore, we first have to identify all *dataflows*. A dataflow describes the exchange of data from one actor to another (or more) actor(s). The transferred data not only consist of the actual message but also of metadata (see the "Communication in the digital age" section). Both, content and metadata, must be completely identified within our model because both determine privacy. Within our model, each dataflow is labeled along the independent dimensions of *active versus passive* and *intentional versus unintentional* (see the "Communication in the digital age" section).

The modeling of dataflows is well-established in computer science with a variety of tools available. Dataflows can be modeled by means of Dataflow-Diagrams (DeMarco, 1979) or Petri Nets (Petri, 1962). Therefore, our model can be integrated and operationalized in the SDLC and thus, helps enable privacy by design. Furthermore, data can be used to derive information (see the "Communication in the digital age" section). There can be a gap between the data that the sender intended to disclose, and the information that others can draw from it. In the Internet and in times of Big Data analytics, this gap is even amplified due to (a) the power of the underlying data mining algorithms, (b) the computational power of the hardware, and (c) the data's availability, accessibility, and unpredictable future uses (Mayer-Schönberger and Cukier, 2013: 98–122). This conflict line is addressed in our model by correlating the data that is transmitted with the information that can be derived (for an example, see the "Privacy online—use case" section).

Protection needs

The *protection needs* represent a variety of psychological, social, political, and legal requirements that are important to protect. On a very abstract level, three *protection needs* can be identified: the integrity of the person, the integrity of the communication, and the integrity of the social organizations (including democracy as a whole). The *integrity of a person* refers to what Alan Westin has called the four functions of privacy. That is, privacy should preserve personal autonomy, emotional release, self-evaluation, as well as limited and protected communication (Westin, 1967: 32–38). The *integrity of communication* must not be established only for individual reasons, but also in order to protect the communicated information from being exposed to the public. The *integrity of social organizations* refers to the functions that privacy can fulfill for groups or the democratic system as a whole (see the "Social and political science" section).

Traditionally, protection needs mostly referred to the right to protection of personal data, the right to protection of personal life, the right to free speech, and the right to anonymity (Bäumler and Von Mutius, 2003). With the increasing digitization, the social and political dimensions of privacy have come to the fore, which is why new protection needs emerge that extend existing ones. These include the protection of privacy as a basis for communicative freedom, as a basis for democratic publicity, as a means for political resistance, and as a common good (see the "Social and political science" section). In addition, this also includes the protection of trust as a precondition of privacy (see the "Legal sciences" section). With this new perspective on privacy, we need to review existing requirements.

In addition, protection needs vary within different communication contexts. In light of our understanding of communication, which, for example, includes computer-computer-communication and human-computer-communication, the varying nature of protection needs becomes even more relevant. According to action theory, there are also dimensions of implicit knowledge, which need to be taken into account (Stahl, 2016). These dimensions determine norms regulating social interaction in different contexts, which prescribe reasonable expectations about information flow and confidentiality (Nissenbaum, 2009).

Threat and risk analysis

It has to be ensured that the specified protection needs are fulfilled. This necessitates a *threat and risk analysis* which is well-established for IT security (ISO/IEC 27005:2018, 2018). Adopting and applying these procedures is one building block of privacy by design (Spiekermann-Hoff, 2012).

The general analysis process is described in Grimm et al. (2014) and includes that all threats have to be identified and quantified by their risk. *Threats* originate from conflicting interests between actors, and they manifest when weaknesses of the IT system and their embedding organization are exploited. In case of e-mail, it can be assumed that sender and recipient are interested in private communication, while in contrast, third parties such as Google have the interest to collect, save, and process as much data as possible in order to improve their user profiles (and thus their profit). In the IPCM (and also in ISO/IEC 15408:2009, 2009), all threats have to be identified. For each threat it has to be analyzed which protection need is violated, which interests motivate the threat, and which weaknesses are exploited.

Furthermore, threats must be quantified by their *risk*, which is defined as the product of (a) probability of occurrence and (b) amount of damage. Here, damage refers to the violation of the integrity of a particular context. While a quantitative amount of damage can be estimated with respect to the economic value of the data, a quantification of damage in regard to fundamental rights is very hard to estimate and demands deeply grounded qualitative research.

Protection enforcement

The *protection enforcement* describes how the previously specified protection needs are or need to be realized. One determinant is the *type of the protection enforcement*. Privacy requirements can be enforced by different measures, including technical, legal, and/or organizational means. Only by combining all of these, privacy can be achieved.

The other determinant of the protection enforcement is the *type of risk regulation*. Risk can be technically regulated in three ways: (a) Users control the enforcement of the protection needs by themselves, for example, by using self-data protection techniques (*individual control*). (b) Users have *no* control, but trust the involved actors and their good conduct (*trust*). According to Mayer et al. (1995), trust can be described as the willingness of a trustor to take a risky action in a context that he does not fully control, in the expectation that the trustee will control it and protect the trustor in it. (c) Users do not trust the involved actors and thus transfer the enforcement of the protection needs to others, for example, by using system-data protection techniques (*delegated control*). It has to be noted that in practice these three types do not occur in isolation, often they are combined. Trust and delegated control require a third party to execute effective control of the dataflows in the interest of the individuals. From our European legal perspective, this third party would have to be the state or the (European Union) EU, as far as it is obliged to effectively guarantee online privacy not only by omitting unlawful interferences but also by active protection enforcements (Gusy et al., 2016). This third party can effectively safeguard these three control regimes by means of legislation, executive authority, and jurisprudence. From a technical point of view, this trusted third party can be, for example, research institutes, non-governmental organizations who provide corresponding tools such as the Tor-browser or the P3P-Plugin, or private companies acting in the user's interests.

Privacy online—use case

In what follows, we show how our theoretical model can be applied. Let us imagine that two people named Alice and Bob want to meet. First, they make an appointment via e-mail. Alice uses the free webmailer Gmail, Bob uses Yahoo. Afterwards they buy a train ticket online, pay with debit card and Paypal, and store the ticket digitally in an App provided by the railway company. The ticket inspection is done by scanning the ticket's QR code, which is validated on the railway company's server. When on the train, Alice and Bob spend their time online, for example, browsing the WWW using the WiFi provided by the railway company.

Communication context

In the use case, the e-mail exchange is active and intentional. Alice and Bob each act as sender and recipient of the messages. Both use an e-mail-provider (EMP) and an Internet access provider (IAP). Hence, there are several third parties involved, including Gmail, Yahoo, Paypal, and the Railway Company. The more Alice and Bob act online, the more actors got involved. Except Alice and Bob all actors belong to the domain "services":

> Characteristic 1: There is a higher number of involved actors than intended.

The e-mails Alice and Bob exchange contain the actual message and metadata. These data can be interpreted to derive Information. Specifically, the *e-mail content* includes information about, for example, mother tongue, level of education, type of relationship with recipient, and/or language patterns (which can effectively be used for user identification, Iqbal et al., 2010). The *e-mail header* specifies the sender, the recipient, date, and how much is communicated (volume). In addition, the subject line also gives hints on the topic of the conversation. Although Alice and Bob could theoretically hide the e-mail content by means of end-to-end-encryption,[7] it is never possible to hide the e-mail header.

When they use the browser, *HTTP header* gives information on their operating system, resolution, and type and version of the browser *(User-Agent*). It can be used for web tracking by means of browser fingerprinting, personalized advertizing, and/or personalized pricing (e.g. making assumptions on how technophile or well-funded someone is; e.g. latest iPhone vs older PCs). The IP address may be used for geo-localization and may give hints about the users' affiliation with an organization or company. To be able to use the free webmailer, Alice and Bob registered as users. Their *account data* includes their first and last name, birthdate, and address. From their names, further information about their nationality or marital status can be retrieved. The address allows to draw conclusions about their financial and social status.

Their accounts hence enable to link all the exchanged data to their identity and to establish user profiles which reflect the full history of e-mails. Thus, it enables the analysis of communication patterns, for example, length of content, frequency of e-mails, recurring communication partners, time slots:

> Characteristic 2: (Meta) data is comprehensive, rich in information, and easily accessible. The more data is collected, the better the resulting profile becomes, which makes the profile more valuable and the user less private.

All dataflows for the given scenario are depicted in Petri net notation in Figure 3. The example shows that vast amounts of data are being transferred, mostly passively. However, many people are not aware of this passive outcome, because their active contribution do not highlight such transfers. These passive and also unintended dataflows may undermine the user's reasonable expectation to be private, which in turn decreases the level of user's control. Furthermore, most of the passive data flows to service providers:

> Characteristic 3: There is a discrepancy between active and passive as well as intended and unintended dataflows. Thereby, passive dataflows almost always correlate with unintended dataflows. This imbalance can result in privacy violations.

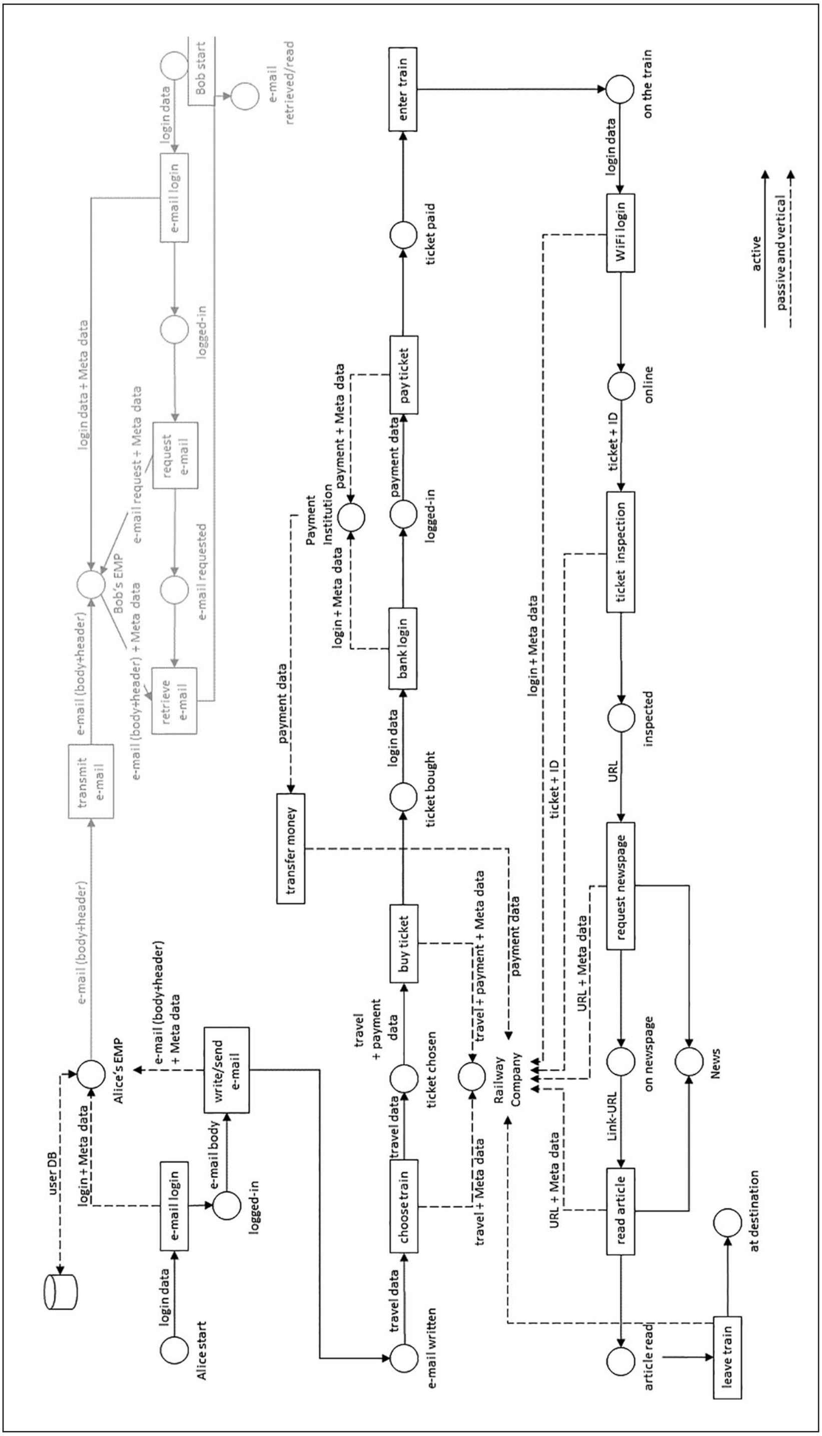

Figure 3. Dataflows for the online scenario of the use case.

Protection needs

The given example affects the *integrity of the person*, in particular, the need for limited and protected communication. Assuming that the communicated information would not be relevant to only Alice and Bob but also to their friends and families, this represents an infringement of the *integrity of communication*. At the same time, there is much information passively communicated that can be processed and used in order to restrain the personal autonomy of Alice and Bob. Moreover, if the communication between Alice and Bob was of political or economic relevance, also the *integrity of organizations* would be concerned.

Alice and Bob need to communicate in order to meet in person. Being able to communicate hence necessitates the first and primary protection need. More specifically, as their communication took place using e-mail, they need their e-mail communication to be protected from unwanted access of other actors and network components.

The factual capacity to execute this right has become dubious under the aforementioned conditions of online communication contexts (see the "Communication context" section). Online communication requires individuals to disclose their data not only to their communication partners but also to unintended third parties. These third parties in general possess more power than the users, creating a power asymmetry that through gaining access to data increases continually. Given these increased power asymmetries, privacy as an individual right to self-determination is no longer sufficient (Cohen, 2012: Chapters 5–6). Accordingly, the distinction between *private* and *public information* can no longer exclusively be drawn by individuals alone. Publicity and privacy increasingly fall together, and protection needs have to focus on the interplay between these two spheres and the social and political consequences that result from this interplay:

> Characteristic 4: Protection needs must include not only active but also passive dimensions of the communication process.

Threat and risk analysis

As a complete threat and risk analysis would go beyond the scope of this article, it is exemplarily done for one threat derived from the given use case, namely *Web tracking*. Web tracking denotes any kind of tracing of user's activities on the web. Thereby, characteristics of the WWW are exploited, namely cookies and/or browser fingerprinting.

"Free" e-mail services like Gmail or Yahoo illustrate how new business models have been established. Users do not pay with money but with their data. While this describes the conflicting interests of the involved actors on a superordinate level, this conflict is reflected on the data level as well. The use of HTTP header for responsive design may be a legitimate purpose, while its usage for Web tracking by means of browser fingerprinting is not. Often purposes are intentionally obfuscated by service providers, for example, by using intentionally vague terms like "service optimization" in the privacy statement.

The extensive coverage of Web trackers allows to comprehensively monitor and analyze user behavior. Therefore, the likelihood of Web tracking being privacy-invasive is apparent. Moreover, there is not a diversification but a monopolization of Web tracking (Wambach and Bräunlich, 2016). As the Internet is a decentralized global communication infrastructure, there is no cartel law that can prevent such monopolization, which creates a new power structure, also called *platformization* (Srnicek, 2016). Hence, from a democratic standpoint, the impact of Web tracking is concerning. Platform dynamics "require" to use certain applications on the providers' terms of privacy protection, even though these terms are not written in the users' best interest (Fernback and Papacharissi, 2007). This threatens democratic values of freedom and equality.

According to ISO/IEC 15408:2009 (2009), due to the high likelihood and high impact of Web tracking, the overall risk of Web tracking can be considered as critical (see "Threat and risk analysis" subsection in section "The interdisciplinary privacy and communication model"):

> Characteristic 5: Current business models amplify conflicts of interests between users and service providers, and, thereby increase privacy risks and threaten fundamental values.

Protection enforcement

Considering the impact of Web tracking on privacy, effective countermeasures against it need to be implemented. On the *technical* side, the risk of Web tracking can be reduced by self-data protection tools such as Ghostery or PrivacyBadger. On the *legal* side, the General Data Protection Regulation (GDPR) and the ePrivacy Regulation (ePR) determine how cookies can be set and processed lawfully. Assuming that it is the service provider's interest to act lawfully, GDPR and ePR influence their cookie policy and thus, reduce the risk of Web tracking.

For an effective protection against Web tracking it is indispensable to investigate how risk is regulated (see the "Protection enforcement" subsection in section "The interdisciplinary privacy and communication model"). With respect to *individual control*, the users can protect themselves against Web tracking by using the above-mentioned self-data protection techniques. In this context, it is useful to make people aware of the vast amounts of data by means of Web tracking. Increased awareness could be achieved by including graphical visualization into browsers such as Lightbeam or by sending users respective alerts when a service provider's privacy policy does not match the privacy settings such as done by P3P.

However, being too overwhelming, the protection cannot be burdened on users alone. In addition, in the case of Web tracking, the possibilities to perform control are restricted. These limited possibilities of control must be intercepted by the protection of trust (see the "Social and political science" section). The user's trust hence needs to be protected by the state or EU by means of a legislation which restricts and regulates the use of cookies and Web tracking. Considering delegated control, users can transfer the enforcement and thus, delegate control to a trusted third party, for example, the Tor-browser, which protects against Web tracking. However, several of these solutions still lack practicability (e.g. Tor with respect to performance and usability):

> Characteristic 6: Privacy protection cannot be burdened on users alone.

Conclusion

In this article, we combine the perspectives from communication science, computer science, social and political science, and legal sciences on privacy in the digital age aiming to contribute to a deeper systematization and understanding of the complex concept of privacy. The result is an IPCM, which connects the perspectives of four disciplines into one overarching theoretical model.

Our IPCM is configured to operationalize attempts to study privacy in the digital age, so that it can be transferred and used for concrete examples. In our use case, we identified six characteristics typical for contemporary communication, which evidence several privacy turbulences. These privacy turbulences illustrate two important consequences: First, the protection of privacy cannot be burdened on the users alone but must include product development, service providers, law, and policy makers. Second, an understanding of privacy protection as common democratic challenge needs to gain grounds, which implies a politization of privacy. This performatively leads to an understanding according to which privacy is not only of relevance for individuals and their personal autonomy but also for the functioning of democratic systems (Bennet, 2015; Helm and Eichenhofer, 2019; Seubert and Helm, 2017). This new, more encompassing view on privacy warrants appropriate socio-political reactions. Specifically, this could mean a supra-national regulation model that goes beyond the GDPR, first by expanding across the borders of the EU and second by taking into account the structural threats which derive from meta-data analytics and platform dynamics. Those threats systematically disadvantage underprivileged groups of people (Eubanks, 2018), thus increasing existing power asymmetries.

Because our primary concern was to bring together several interdisciplinary perspectives, it was not possible to elaborate on several aspects in detail. For example, the precise method-based embedding of the IPCM into the SDLC needs to be elaborated. This implies the concretization of the modeling process throughout all phases of the SDLC. Without claim of completeness, this includes, for example, connecting the model with requirements engineering or risk assessment procedures (such as ISO/IEC 27005:2018, 2018 or IEEE 29148-2018, 2018), modeling languages such as Dataflow-Diagrams (DeMarco, 1979), identification of patterns and best practices,[8] or the integration into evaluation and certification standards such as Common Criteria ISO/IEC 15408:2009 (2009) and/or ISO/IEC 27000:2018 (2018).

Technologically, protection needs are identified, designed, and implemented according to standardized processes such as IEEE 29148-2018 (2018). However, any attempt to solve the multidimensional concept of privacy only technologically is predicted to fail. Value sensitive design (VSD) (Friedman et al., 2013) seems promising to bridge this gap. Besides several overlapping points, most apparently VSD provides a methodology to elucidate design requirements according to moral and ethical values. Thereby, VSD reflects the multilateral approach of the IPCM (actors and stakeholders, “Communication context” section; value tensions and threats, “Threat and analysis” section).

Further research is also needed concerning privacy risk assessment, especially with respect to the amount and quality of damage effected by privacy turbulences in regard to fundamental democratic rights of freedom and equality.

In addition, all disciplines compromised on a number of epistemological notions and perspectives. For example, in qualitative social and political science, modeling is uncommon. We therefore do want to emphasize the performative dimension of modeling by raising awareness for the fact that we do understand our model to be a *prescription* of reality rather than a *description* of it, and that we understand it to be situated in a specific cultural background (Europe) and a specific political system (liberal democracy). However, developing a common language and focusing on a common ground was more important to us than insisting on epistemological differences. We hope our model and the results of our analysis present a useful basis for further and more detailed mono- and interdisciplinary endeavors to address the challenges of privacy protection in the digital age.

Acknowledgements

All authors have agreed to the submission and the article is not currently being considered for publication by any other print or electronic journal.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Volkswagen Stiftung, project "Transformations of privacy".

ORCID iDs

Katharina Bräunlich https://orcid.org/0000-0002-9664-4809
Paula Helm https://orcid.org/0000-0002-2719-9721

Notes

1. Synonyms are seclusion, withdrawal, confidentiality, or secrecy.
2. Often used as synonyms: control of information, flow of information, or informational self-determination.
3. https://www.eff.org/issues/anonymity (accessed 6 November 2019).
4. For a detailed analysis of the relationship of privacy and data protection, see Eichenhofer (2016) and Gusy (2018).
5. https://www.torproject.org/ (accessed 7 November 2019).
6. In qualitative social and political science, modeling is rather uncommon. Nevertheless, for the purpose of this article, it seems to be an appropriate method. A critical reflection of this approach is discussed in "Conclusion" section of this article.
7. Notably, there is no built-in end-to-end-encryption in Gmail (and most other free Webmailers as well). Instead, it has to be integrated via external (and in most cases, not supported) add-ons.
8. For a collection of such patterns, see for example, https://privacypatterns.org/patterns/ (accessed 11 November 2019).

References

Altman I (1975) *The Environment and Social Behavior*. Monterey, CA: Brooks Cole.

Androulaki E, Karame GO, Roeschlin M, et al. (2013) Evaluating user privacy in Bitcoin. In: Sadeghi AR (ed.) *Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, Vol. 7859*. Berlin; Heidelberg: Springer, pp. 275–292.

Bäumler H and Von Mutius A (2003) *Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts*. Berlin: Vieweg+Teubner Verlag

Becker C and Seubert S (2016) Privatheit, kommunikative Freiheit und Demokratie. *Datenschutz und Datensicherheit—Dud* 40(2): 73–78.

Bennet C (2015) *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.

Betancourt M (2016) *The Critique of Digital Capitalism: An Analysis of the Political Economy of Digital Culture and Technology*. Brooklyn, NY: punctum books.

boyd d (2014) *Its Complicated: The Social Life of Networked Teens*. New Haven, CT: Yale University Press.

Bozdag E and Van den Hoven J (2015) Breaking the filter bubble: democracy and design. *Ethics and Information Technology* 17: 249–265.

Bygrave L (2014) *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press.

Cavoukian A (2009) Privacy by design—the 7 foundational principles. Available at: https://www.ipc.on.ca/wpcontent/uploads/Resources/7foundationalprinciples.pdf (accessed 18 July 2018).

Chugh R (2012) Social networking for businesses: is it a boon or bane? In: Cruz-Cunha MM, Putnik GD, Lopes N, et al. (eds) *Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions*. IGI Global. Available at: https://bit.ly/2Y1IIcP (accessed 10 December 2019).

Cohen J (2012) *Configuring the Network Self. Law, Code and the Play of Everyday Practice*. New Haven, CT: Yale University Press.

Danezis G, Dingledine R and Mathewson N (2003) Mixminion: design of a Type III anonymous remailer protocol. In: *Proceedings of the IEEE symposium on security and privacy*, Berkeley, CA, 11–14 May, pp. 2–15. New York: IEEE.

DeMarco T (1979) *Structured Analysis and System Specification*. Upper Saddle River, NJ: Prentice Hall.

Dienlin T (2014) The privacy process model. In: Garnett S, Halft S, Herz M, et al. (eds) *Medien und Privatheit*. Passau: Karl Stutz, pp. 105–122.

Dienlin T and Metzger MJ (2016) An extended privacy calculus model for SNSs—analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication* 21(5): 368–383.

Eichenhofer J (2016) Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz. *Der Staat* 55: 41–67.

Eubanks V (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

Fernback J and Papacharissi Z (2007) Online privacy as a legal safeguard: the relationship among consumer, online portal and privacy policies. *New Media & Society* 9(5): 715–734.

Friedman B, Kahn PH, Borning A, et al. (2013) Value sensitive design and information systems. In: Doorn N, Schuurbiers D, van de Poel I, et al. (eds) *Early Engagement and New Technologies: Opening Up the Laboratory* (Philosophy of Engineering and Technology), vol. 16. Dordrecht: Springer, pp. 55–95.

Grimm R and Delfmann P (2017) *Digitale Kommunikation*. Berlin: De Gruyter.

Grimm R, Simic-Draws D, Bräunlich K, et al. (2014) Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. *Informatik-spektrum* 39(1): 2–20.

Gusy C (2018) Datenschutz als Privatheitsschutz oder Datenschutz statt Privatheitsschutz? *Europäische Grundrechte-zeitschrift* 45: 244–254.

Gusy C, Eichenhofer J and Schulte L (2016) e-Privacy. Von der Digitalisierung der Kommunikation zur Digitalisierung der Privatsphäre. *Jahrbuch des öffentlichen Rechts der Gegenwart* 64: 385–410.

Habermas J (1995) *Theorie Kommunikativen Handeln, Bd. 2, Kap. V, FFM*. Frankfurt am Main: Suhrkamp.

Hansen M, Schwartz A and Cooper A (2008) Privacy and identity management. *IEEE Security & Privacy* 6(2): 38–45.

Haraway D (1988) Situated knowledges: the science question in feminism and the privilege of partial perspective. *Feminist Studies* 14(3): 575–599.

Hartzog W and Richards N (2016) Taking trust seriously in privacy law. *Stanford Technology Law Review* 19: 431–472.

Helm P and Eichenhofer J (2019) Reflektionen zu einem social turn in den privacy studies. In: Henning M (ed.) *Privatheit und Digitalisierung*. Bielefeld: Transcript, pp.139–165.

Helm P and Seubert S (2020) Normative paradoxes of privacy: literacy and choice in platform societies. *Surveillance & Society* 18(2): 185–198.

IEEE 12207-2017 (2017) Systems and software engineering—software life cycle processes. Available at: https://standards.ieee.org/standard/12207-2017.html

IEEE 29148-2018 (2018) ISO/IEC/IEEE international standard—systems and software engineering—life cycle processes—requirements engineering. https://standards.ieee.org/standard/29148-2018.html

IETF RFC 1122 (1989a) Requirements for internet hosts —communication layers. Available at: https://tools.ietf.org/html/rfc1122 (accessed 10 January 2019).

IETF RFC 1123 (1989b) Requirements for internet hosts—application and support. Available at: https://tools.ietf.org/html/rfc1123 (accessed 10 January 2019).

Iqbal F, Binsalleeh H, Fung BCM, et al. (2010) Mining writeprints from anonymous e-mails for forensic investigation. *Digital Investigation* 7(1–2): 56–64.

Isin E and Ruppert-Schulze E (2015) *Being Digital Citizens*. Lanham, MD: Rowman & Littlefield International.

ISO/IEC 15408:2009 (2009) Common criteria for information technology security evaluation, and common methodology for information technology security evaluation.

ISO/IEC 27000:2018 (2018) Information technology—security techniques—information security management systems—overview and vocabulary.

ISO/IEC 27005:2018 (2018) Information technology—security techniques—information security risk management.

Laufer RS and Wolfe M (1977) Privacy as a concept and a social issue: a multidimensional developmental theory. *Journal of Social Issues* 33(3): 22–42.

Luhman N (1988) *Soziale Systeme. Grundriss Einer Allgemeinen Theorie*. Frankfurt am Main: Suhrkamp.

Marwick A and boyd d (2014) Networked privacy: how teenagers negotiate context in social media. *New Media & Society* 16(7): 1051–1067.

Masur PK (2018) *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments*. Cham: Springer.

Mayer RC, Davis JH and Schoorman FD (1995) An integrative model of organizational trust. *Academy of Management Review* 20: 709–734.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: Hodder & Stoughton.

Merten K (1977) *Kommunikation: Eine Begriffs- und Prozeßanalyse*. Opladen: Westdeutscher Verlag.

Nissenbaum H (2009) *Privacy in Context. Technology, Policy and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Petri CA (1962) *Kommunikation mit Automaten*. PhD Thesis, Technische Hochschule Darmstadt, Darmstadt.

Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.

Pfitzmann A and Köhntopp M (2001) Anonymity, unobservability, and pseudonymity—a proposal for terminology. In: Federrath H (ed.) *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science 2009*. Berlin; Heidelberg: Springer, pp. 1–9.

Prakke H (1968) *Kommunikation der Gesellschaft: Einführung in die funktionale Publizistik*. Münster: Verlag Regensberg.

Regan P (2002) Privacy as a common good in the digital World. *Information, Communication and Society* 5(3): 382–405.

Rössler B (2001) *Der Wert des Privaten*. Frankfurt am Main: Suhrkamp.

Ruj S, Stojmenovic M and Nayak A (2012) Privacy preserving access control with authentication for securing data in clouds. In: *Proceedings of the 2012 12th IEEE/ACM international symposium on cluster, cloud and grid computing (CCGrid 2012)*, Ottawa, ON, Canada, 13–16 May, pp. 556–563. New York: IEEE.

Schneier B (1996) *Applied Cryptography*. 2nd ed. Hoboken, NJ: John Wiley & Sons.

Seubert S and Helm P (2017) Privatheit und Demokratie. Forschungsjournal Soziale Bewegungen. *Sonderschwerpunkt Privatheit und Demokratie* 30:120–123.

Solove DJ (2008) *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Spiekermann-Hoff S (2012) The challenges of privacy by design. *Communications of the ACM* 55(7): 34–37. Available at: https://epub.wu.ac.at/5494/ (accessed 7 November 2019).

Srnicek N (2016) *Platform Capitalism*. Cambridge: Polity Press.

Stahl T (2016) Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology* 18(1): 33–39.

Sundar SS, Kang H, Wu M, et al. (2013) Unlocking the privacy paradox: do cognitive heuristics hold the key? In: *Proceedings of the CHI EA 2013—extended abstracts on human factors in computing systems: changing perspectives*, Paris, 27 April–2 May, pp. 811–816. New York: Association for Computing Machinery.

Trepte S (2020) The social media privacy model: privacy and communication in the light of social media affordances. *Communication Theory*.

Trepte S and Reinecke L (2011) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. New York: Springer.

Van Den Berg PEW, Arentze TA and Timmermans HJP (2012) New ICTs and social interaction: modelling communication frequency and communication mode choice. *New Media & Society* 14(6): 987–1003.

Wambach T and Bräunlich K (2016) The evolution of third-party web tracking. In: Camp O, Furnell S and Mori P (eds) *Information Systems Security and Privacy (2nd International Conference on ICISSP 2016*, Rome, Italy, 19–21 February 2016). New York: Springer, pp. 130–147.

Warner M (2002) *Publics and Counterpublics*. Cambridge: Zone Books.

Warren SD and Brandeis LD (1890) The right to privacy. *Harvard Law Review* 4(5): 193–220.

Wessels B (2012) Identification and the practices of identity and privacy in everyday digital communication. *New Media & Society* 14(8): 1251–1268.

Westin A (1967) *Privacy and Freedom*. New York: Atheneum Press.

Author biographies

Katharina Bräunlich is a postdoctoral researcher at the Department of Computer Science at the University of Koblenz and Landau. Her research focuses on IT security and privacy.

Tobias Dienlin is a postdoctoral researcher at the Department of Media Psychology at the University of Hohenheim in Germany. His research is focused on privacy, well-being, and social media.

Johannes Eichenhofer is a postdoctoral researcher at the University of Bielefeld (Germany), Faculty of Law. His research is focused on human rights and administrative law, especially in the fields of privacy, data protection, and migration and integration.

Paula Helm, is a postdoctoral fellow in the research project "Structural Transformations of Privacy" at the University of Frankfurt/Main. Her main research focuses on the social conditions of addiction therapy, privacy, anonymity and cultures of disconnection.

Sabine Trepte has been a full professor since March 2013 at the University of Hohenheim and chairs the Department of Media Psychology. Her main research in the field of media psychology focuses on privacy and self-disclosure in the social web.

Rüdiger Grimm is an emeritus professor of Computer Science at the University of Koblenz and Landau, currently engaging as scientific advisor and ombudsman for good scientific practice at the Fraunhofer Institute for Secure Information Technology (SIT).

Sandra Seubert has been professor of Political Science since 2009 at the Goethe University Frankfurt. She works on questions of democratic theory, in particular, of shifting boundaries between privacy and public under conditions of digitization of communication as well as theories of transnational and European citizenship.

Christoph Gusy is professor of Public Laws, Political Theory, and Constitutional History (since 1993). His main research focuses on the Weimar Republic, human rights, security affairs, and data protection.