COGITATIO

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 2, Pages 258–269
DOI: 10.17645/mac.v8i2.2855

Article

How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information

Philipp K. Masur

Department of Communication, Johannes Gutenberg University Mainz, 55128 Mainz, Germany;
E-Mail: philipp.masur@uni-mainz.de

Submitted: 30 January 2020 | Accepted: 18 March 2020 | Published: 23 June 2020

Abstract
Current debates on online privacy are rooted in liberal theory. Accordingly, privacy is often regarded as a form of freedom from social, economic, and institutional influences. Such a negative perspective on privacy, however, focuses too much on how individuals can be protected or can protect themselves, instead of challenging the necessity of protection itself. In this article, I argue that increasing online privacy literacy not only empowers individuals to achieve (a necessarily limited) form of negative privacy, but has the potential to facilitate a privacy deliberation process in which individuals become agents of social change that could lead to conditions of positive privacy and informational self-determination. To this end, I propose a four-dimensional model of online privacy literacy that encompasses factual privacy knowledge, privacy-related reflection abilities, privacy and data protection skills, and critical privacy literacy. I then outline how this combination of knowledge, abilities, and skills 1) enables to individuals to protect themselves against some horizontal and vertical privacy intrusions and 2) motivates individuals to critically challenge the social structures and power relations that necessitate the need for protection in the first place. Understanding these processes, as well as critically engaging with the normative premises and implications of the predominant negative concepts of privacy, offers a more nuanced direction for future research on online privacy literacy and privacy in general.

Keywords
data protection; digital literacy; information society; informational self-determination; new media; online privacy

Issue
This article is part of the issue "The Politics of Privacy: Communication and Media Perspectives in Privacy Research" edited by Johanna E. Möller (Johannes Gutenberg University Mainz, Germany), Jakub Nowak (Maria Curie-Sklodowska University, Poland), Sigrid Kannengießer (University of Bremen, Germany) and Judith E. Möller (University of Amsterdam, The Netherlands).

1. Introduction

In all societies, people seek privacy from time to time (Altman, 1975; Moore, 1984; Westin, 1967). But privacy is not an end in itself. Instead, it describes conditions under which fundamental needs such as autonomy, emotional release, self-development, and self-evaluation can be satisfied (Trepte & Masur, 2017; Westin, 1967). The value of privacy is thus acknowledged in many declarations of human rights—either explicitly or indirectly deduced from more fundamental rights that privacy helps to achieve.

Although concepts of privacy can be traced back to different schools of thought, contemporary discussions of online privacy almost exclusively adopt a perspective that is rooted in liberal theories (e.g., Hobbes, 1651; Mill, 1859/2015). In trying to grasp and describe current threats to privacy such as ubiquitous surveillance and large-scale data collection (Greenwald, 2014), the increasing commodification of information (Sevignani, 2016), the blurring of public and private in networked environments (Masur, 2018b), and the corresponding malleability of the individual by powerful economic players (Acquisti, Brandimarte, & Loewenstein, 2015), privacy

scholars and the public alike conceive of privacy, in one way or the other, as a form of protection against social, economic, or institutional interferences. This perspective resembles the notion of 'negative freedom' (Berlin, 1969). Variants of such a negative conception of privacy can be found in non-intrusion theories of privacy (e.g., Warren & Brandeis, 1890), seclusion theories of privacy (e.g., Gavison, 1980; Westin, 1967), as well as in control and limitation theories of privacy (e.g., Altman, 1975; Miller, 1971; Rachels, 1975; Tavani, 2007).

By viewing privacy as defense against intrusion and external influences, it is not surprising that prominent research questions ask how and whether individuals can protect themselves or can be protected in an increasingly privacy-invasive media environment (e.g., Baruh, Secinti, & Cemalcilar, 2017; Park, 2013), how privacy concerns relate to privacy protection behaviors (for overviews, see e.g., Barth & de Jong, 2017; Kokolakis, 2017), or how policies, laws, or regulations should be formulated in order to protect individuals' privacy (e.g., Gutwirth, Leenes, & de Hert, 2015, 2016).

In these liberal discourses on privacy, the focus is protection against access to and identification of the individual. Therefore, proposed solutions include, but at the same time are limited, to strengthening individuals' knowledge, skills and abilities to protect themselves (e.g., Park, 2013; Trepte et al., 2015) and the implementation of privacy and data protection regulations and laws on the policy level (Solove & Schwartz, 2019). From a critical point of view, these solutions must be regarded as a consequence of the predominant negative perspective on privacy. Similar to thinking that building a bunker is the best solution in times of war, they fail to challenge the system itself. Such solutions only provide remedies against the most visible and tangible consequences of a status quo that slowly erodes the value of privacy. Similar to treating only the symptoms of a disease instead of its causes, providing protection against novel intrusions fails to acknowledge that the necessity for such protection is a consequence of the social power relations that brought about the risks and intrusions in the first place.

Scholars have already noted that negative accounts of privacy fail to grasp the threats of today's technology-driven societal and economic dynamics (Fuchs, 2011, 2012; Seubert & Becker, 2019; Stahl, 2016). One argument is that societal structures that favor the commodification of information (cf. Sevignani, 2016; Zuboff, 2019) and support an imbalance between large economic players and individuals do not only represent external threats to individuals' privacy in that they implement ubiquitous monitoring as well as large-scale data collection. Moreover, these structures (and the economic players that build them) are also constituent of what spaces of privacy exist at all and how these spaces can be achieved and protected. More specifically, they cause inner threats to privacy as individuals' everyday practices within these spaces perpetuate these structures of domination (Seubert & Becker, 2019). Fuchs (2011) similarly argues that such a liberal notion of privacy "legitimizes and reproduces the capitalist class structure" (p. 231). For example, social network sites provide new means of communication, but at the same time erode boundaries between public and private by flattening traditionally separated contexts into one broad audience (Marwick & boyd, 2011). The same platform then offers 'privacy settings' to protect against the privacy risks resulting from this context collapse (albeit only on the horizontal level; see Masur, 2018b). For the individual, this creates an illusion of privacy (Trepte & Reinecke, 2011) and thereby promotes communication practices (e.g., high levels of information disclosure) that, in turn, support the commodification of information and lead to even more exploitation of personal data on the vertical level.

In a similar way, our research and concepts of privacy are shaped by an uncritical adoption of a negative liberal perspective on privacy. As long as the focus is exclusively placed on understanding how individuals can protect themselves in a world of mass-surveillance and data collection, research fails to challenge this world itself and to envision alternatives that are based on different premises. The concept of informational self-determination, for example, does embody a notion of positive freedom (Berlin, 1969) and may help to envision alternative approaches to privacy: It refers to an individuals' right and ability to decide for themselves, when and within what limits information about himself or herself should be collected, analyzed or communicated to others (cf. also the seminal privacy definition by Westin, 1967). Such a concept acknowledges and emphasizes an individual's agency, self-mastery, and ability to realize his or her own will instead of guaranteeing protection against external influences. In Germany, for example, the right to informational self-determination was deduced from more general human rights (German Constitution, art. 2, §1 in combination with art. 1, §1) after a planned census of the German population in 1983.

The goal of this article is twofold. First, I discuss the role of online privacy literacy in providing individuals with the ability to protect themselves against external social, economic, and governmental influences (alluding to a negative privacy conception). In this regard, online privacy literacy plays an important role in democratic, but even more so in authoritarian societies, in which individuals may be more in need to protect themselves against identification. Second, I explore how societal change towards a more positive notion of privacy (i.e., informational self-determination) might be possible. The main argument is that again online privacy literacy—the often-proposed solution to protect people's privacy against external influences—may also provide the basis for social transformations because it motivates individuals to become agents of social change and to engage in acts of resistance. That said, this deliberation process may be limited to democratic societies in which social transformations through civic engagement are possible. In authori-

tarian regimes such safe avenues for public deliberation may not be feasible.

In what follows, I will first introduce an extended model of online privacy literacy which includes three basic dimensions: 1) factual privacy knowledge, 2) privacy-related reflection ability, and 3) privacy and data protection skills, and theorizes an overarching dimension called critical privacy literacy. Subsequently, I will analyze the role of online privacy literacy 1) in empowering individuals to protect themselves against institutional and economic interferences and 2) in promoting critical evaluations of the status quo and, in turn, motivate societal change.

2. An Extended Model of Online Privacy Literacy

Prior research on online privacy literacy was often motived by what can be termed the 'knowledge gap hypothesis' (Trepte et al., 2015, p. 339). After the puzzling observation that individuals' concerns about their online privacy did not translate into privacy-related behaviors (cf. the 'privacy paradox'; Barnes, 2006; Barth & de Jong, 2017), it was assumed that the discrepancy between concerns and behaviors could be explained by a lack of knowledge and skills that prevents individuals from engaging in privacy protection practices. Empirical studies hence investigated the relationship between various concepts of privacy literacy and information disclosure or privacy protection strategies (Bartsch & Dienlin, 2016; Masur, Teutsch, & Trepte, 2017; Park, 2013). First theoretical accounts of online privacy literacy often included only one or two dimensions primarily focusing on awareness of economic practices or technical skills (Hoofnagle, King, Li, & Turow, 2010; Park, 2013; Turow, 2003). Only recently, multidimensional models of online privacy literacy that combined these fragmented dimensions emerged from the literature. Trepte et al. (2015) distinguished between factual knowledge, which refers to information about technical, economic, and legal aspects of privacy and data protection, and procedural knowledge, which is understanding data protection strategies.

Building on this four-dimensional knowledge concept, Masur et al. (2017) and Masur (2018a) proposed a comprehensive model of online privacy literacy that aligns more with traditional concepts of literacy by combining various knowledge dimensions and procedural skills with reflection and critical thinking abilities. They argue that knowledge is not sufficient to motivate behavioral and societal change. People need to be able to reflect and question their culture and societal conditions in order to be motivated to drive social transformations (Masur, 2018a, p. 448). In what follows, I present and extend this model (see Figure 1). In doing so, I will differentiate between aspects that pertain to a horizontal (i.e., with regard to other users) and a vertical (i.e., both commercial and institutional) level of privacy (Masur, 2018b; Raynes-Goldie, 2010). All four dimensions are interconnected and built on each other. For example, comprehensive knowledge (e.g., knowing that Facebook collects data from its users to personalize advertisements) is useless without the ability to link this knowledge to one's own behavior (e.g., realizing that disclosing private information contributes to the commodification of information). Similarly, without awareness about horizontal or vertical privacy risks in online environments, procedural knowledge and skills (e.g., knowing how to change privacy settings on a social network sites) are useless.

Furthermore, this model proposes that knowledge, reflection abilities, and skills provide the basis for maximizing individual privacy protection. The overarching dimension of critical privacy literacy hence shifts the focus from the individual to the society as a whole, provide the basis for a critical investigation of the social conditions that necessitate privacy protection and emphasizes the collective nature of privacy (cf. Baruh & Popescu, 2017).

2.1. Factual Privacy Knowledge

This dimension acknowledges that familiarity, awareness, and understanding of facts, concepts, information, and conditions is essential for developing any kind of literacy. Similarly to knowing what a computer looks like and knowing what it can be used for represents a first step towards developing the skills necessary to use it, online privacy literacy fundamentally includes factual knowledge about various social, economic, institutional, technical, and legal aspects of online privacy and data protection.

On the vertical level, factual knowledge includes 1) the awareness and understanding of information flows on the Internet, the economic models of online service providers as well as awareness of their data collection, analysis, profiling, and valorization practices; 2) the awareness and knowledge about governmental and institutional surveillance and monitoring practices; 3) knowledge about technical aspects of data protection and privacy on the Internet (i.e., specific knowledge about the technical infrastructure of the Internet and online applications, privacy-related software as well as the privacy-invasive nature of online applications and platforms); and 4) knowledge about national and international data protection law as well as derivable rights and duties of both companies and users.

On the horizontal level, it includes the awareness and understanding of novel social dynamics that shape and were shaped by networked environments (e.g., social network sites, instant messengers, online shopping platforms) and heighten the risks of privacy violations and intrusions by other users (e.g., scalability, linkability, and editability of information, the convergence of traditionally distinct social contexts, and the blurring of public and private spaces).

2.2. Privacy-Related (Self-)Reflection Ability

The second dimension describes the ability to reflect the knowledge in relation to one's own media use. It encom-

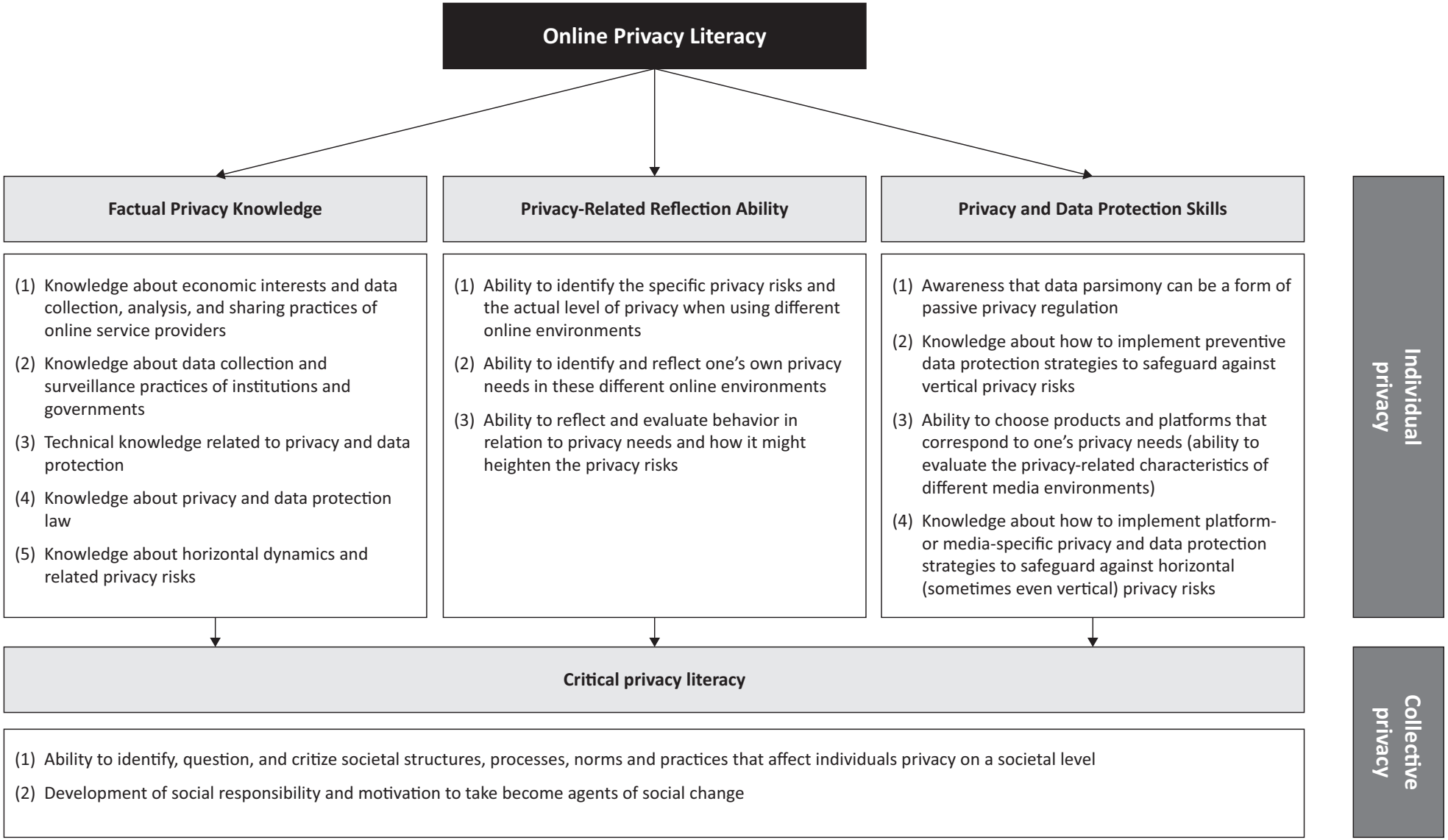

Figure 1. A comprehensive model of online privacy literacy.

passes 1) the ability to identify specific privacy risk that pertain to the self and to evaluate the actual level of privacy in various context and media environments. Based on this assessment, the individual further needs to have 2) the ability to identify his or her privacy needs in these various contexts and media environments in which the outlined horizontal and vertical privacy dynamics occur.

Finally, it includes 3) the ability to reflect one's own behavior and how it might heighten the risk of privacy violations. Although this dimensions still focuses on protecting one's own privacy, these reflection abilities must be regarded as an important requirement for developing more critical evaluations abilities. Only by realizing that one's privacy is at risk in most media environments, the individual develops a more critical understanding of the norms and social structures the affect individuals' privacy in general.

2.3. Privacy and Data Protection Skills

The third dimension builds upon the two previous dimensions in that it consolidates factual knowledge into procedural skills. It represents all skills necessary to implement effective data protection and privacy regulation strategies that safeguard against the horizontal and vertical privacy risks in online environments. In a first step, the individual needs to develop the 1) understanding and awareness that data parsimony (e.g., disclosing less private information) is a fundamental step towards more privacy online.

Further skills include the procedural knowledge of 2) how to implement sophisticated data protection strategies that prevent access and identification on the vertical level (e.g., using anonymization software such as TOR, installing anti-tracking-plugins, or encrypting communication), and 3) how to selectively choose platforms and services that guarantee a higher level of privacy or withdraw from privacy-invasive products. Finally, this dimension also includes 4) the skills necessary to use platform-specific privacy settings to minimize horizontal privacy risks (e.g., restricting access to posts or using pseudonyms).

2.4. Critical Privacy Literacy

The previous three dimensions must be regarded as a basis of online privacy literacy that empower the individual to restrict access to the self, to prevent unwanted identification, and to ensure data protection. As such, they are means to maximize negative privacy, i.e., freedom from external influences. Yet, learning about social, economic, institutional, technical, and legal aspects of online privacy and reflecting one's own media use and privacy-related behavior, as well as trying to protect one's privacy in the various media environments, should eventually lead to an uncertainty about how much protection is actually feasible. This uncertainty, in turn, should lead into a feeling of discomfort about the limited power with regard to minimizing vertical privacy intrusions. As a consequence, several scholars have argued that individuals might develop a form of privacy fatigue (Choi, Park, & Jung, 2018) or privacy cynicism (Hoffmann, Lutz, & Ranzini, 2016). Such concepts refer to a cognitive coping mechanism that, based on uncertainty, mistrust and a feeling of powerlessness, renders privacy protection futile (Hoffmann et al., 2016). However, individuals might also realize that privacy—a space of withdrawal paradoxically shaped by those that they seek protection from—provides them nonetheless with the possibility to distance themselves and reflect on their "interweaving within social practices" which, in turn, might lead to "reflexive redefinition of how to participate in [these] social practices" (Seubert & Becker, 2019, p. 940).

Similarly to critical media literacy (cf. Alvermann & Hagood, 2000; Baacke, 1996; Groeben, 2002; Livingstone, 2004; Potter, 2008), I define 'critical privacy literacy' as the general ability to criticize, question, and challenge existing assumptions about the social, economic, and institutional practices that have led to a status quo in which the individual has to defend his or her freedom against unequally more powerful economic and institutional influences. Critical privacy literacy involves the ability 1) to identify and analyze problematic societal structures, norms, and practices that affect privacy of individuals as part of the larger society. This type of literacy moves the focus from the individual to the society, and it involves the understanding of economic and governmental interests in data collection and processing. It ultimately leads to the ability to challenge such institutional practices from an ethical point of view. An individual that critically engages with privacy-related aspects of society is hence less overwhelmed by a seemingly unchallengeable environment, less likely to develop privacy cynicism (Hoffmann et al., 2016), and able to maintain an autonomous, and rational position.

Being critical further makes individuals more political in that they should increasingly feel 2) the responsibility to change problematic structures, norms, and practices. This responsibility may include taking part in discourses, supporting privacy initiatives, or participating in the democratic society in general. In sum, individuals with high critical privacy literacy are more motivated and competent participants of social life as they know how to use their privacy-related knowledge and skills as instruments of social communication and change.

3. Functions of Online Privacy Literacy

Based on the multidimensional model presented above, the role of online privacy literacy is twofold (cf. Figure 2). On the one hand, it empowers individuals (at least to some degree) to protect themselves against social, economic, and institutional influences. Online privacy literacy allows them to implemented data protection strategies and privacy regulation strategies by themselves (hereinafter called self-data protection) or by 'enforc-

ing' data protection through laws and regulations (hereinafter called legal data protection). On the other hand, online privacy literacy—and in particular critical privacy literacy—can be regarded as a fundamental basis for the realization of citizens' democratic potential and, in turn, as a motivator of societal transformations. In the following, I will discuss both roles in more detail.

3.1. Empowering Individuals to Protect Themselves Against Social, Economic, and Institutional Influences

There is growing body of research that suggests that higher online privacy literacy is linked to more self-data protection (Figure 2, upper panel). For example, Park (2013) conducted a survey with 419 adult Internet users in the US and found that familiarity with technical aspects of online privacy, awareness of institutional surveillance practices, and privacy policy understanding predicted privacy protection behavior (including withdrawal, hiding, and technical data protection strategies). Likewise, Kraus, Wechsung, and Möller (2014) found that more literate smartphone users were more likely to choose encrypted instant messengers (e.g., Threema or Signal). Based on 1,945 German Internet users, Masur et al. (2017) similarly found positive relationships between higher overall online privacy literacy and various data protection strategies (e.g., using pseudonyms or anonymization tools). Finally, a meta-analysis of 10 studies revealed a small, but positive correlation between privacy literacy and the implementation of data protection strategies (Baruh et al., 2017). These findings suggest that fostering particularly the first three dimensions of online privacy literacy, factual knowledge, self-reflection, and procedural skills, are related to more individual data protection. Similar to being able to build a bunker or react reasonably under attack, online privacy literacy seems to provide individuals with the knowledge, abilities, and skills to protect oneself against external influences.

Online privacy literacy may be even more important for citizens in authoritarian societies or hybrid regimes (such as e.g., Russia or Turkey; The Economist Intelligence Unit, 2019) as it provides the knowledge, abilities, and skills to protect oneself against intrusions or surveillance by powerful governments. For example, simply contacting 'suspicious' persons or googling certain information (e.g., to gain an outside perspective one's own government or country) can be risky in a regime that tries to minimize opposition. Knowing how to use TOR (2020) or encrypted messenger such as Signal or Threema can provide safe ways to communicate or surf the Internet.

However, several arguments can be brought forward that challenge the potential of online privacy literacy in protecting individual's privacy. First, most studies cited used cross-sectional survey designs and hence did not investigate causal effects. It remains unclear whether teaching of knowledge and skills actually leads to behavioral changes in individuals or whether knowledge simply increases with the use of data protection strategies (cf. Masur, Teutsch, Dienlin, & Trepte, 2017). Second, others have argued that promoting self-data protection could be an ill-fated solution as almost no implementable tool or strategy is sufficient to protect people's privacy on the vertical level and self-data protection may create undesired effects such as negligence of political responsibility or fostering inequalities between users (Matzner, Masur, Ochs, & von Pape, 2016). It is important to consider the limits of self-data protection for actually protecting individuals' privacy. Matzner (2014), for example, argues that big data and ubiquitous computing involve privacy threats "even for persons about whom no data has been collected and processed" (p. 91). Other research found links between non-members of a social network sites based only on information extracted from friendship and email contact information of their members (Horvát, Hanselmann, Hamprecht, & Zweig, 2012; Sarigol, Garcia, & Schweitzer, 2014). So even individuals who withdraw from using privacy-invasive products or platforms are vulnerable to vertical privacy intrusions.

Furthermore, many scholars have argued that individual data protection is no longer sufficient in networked environments. Instead, users of social network sites and other online environments need to develop group or collective privacy management practices in order to establish information flows within collectively set up boundaries (Marwick & boyd, 2014; Nissenbaum, 2010; Petronio, 2002; Wolf, Willaert, & Pierson, 2014). In the light of this, Baruh and Popescu (2017) have argued that regulatory efforts that center on individual privacy literacy and self-data protection are destined to fail because they fail to acknowledge this collective nature and value of privacy.

Finally, a negative notion of privacy and hence individual protection against external influences only work, if these privacy invasions are readily perceivable and linkable to the individual. Yet, in modern big data environments, vertical privacy violations are mostly intangible (Acquisti et al., 2015). For example, the "algorithmic social sorting characteristic of big data environments drastically limits the ability of individuals to self-define, and thus claim control and agency, over their social trajectory" (Baruh & Popescu, 2017, p. 591). Personalization services (e.g., social network sites, but also online shopping platforms, etc.) put populations into abstract, algorithmically produced categories that "are not only far removed from the 'selfhood categories' individuals might use to define themselves, but also recontextualize the self in a fleeting and unchallengeable manner" (p. 591). In order to question such an information society, the focus needs to shift from the individual to the collective value of privacy.

3.2. Motivating Individuals to Become Agents of Social Change

Media literacy has long been regarded as a fundamental requirement for the diffusion of democratic potentials

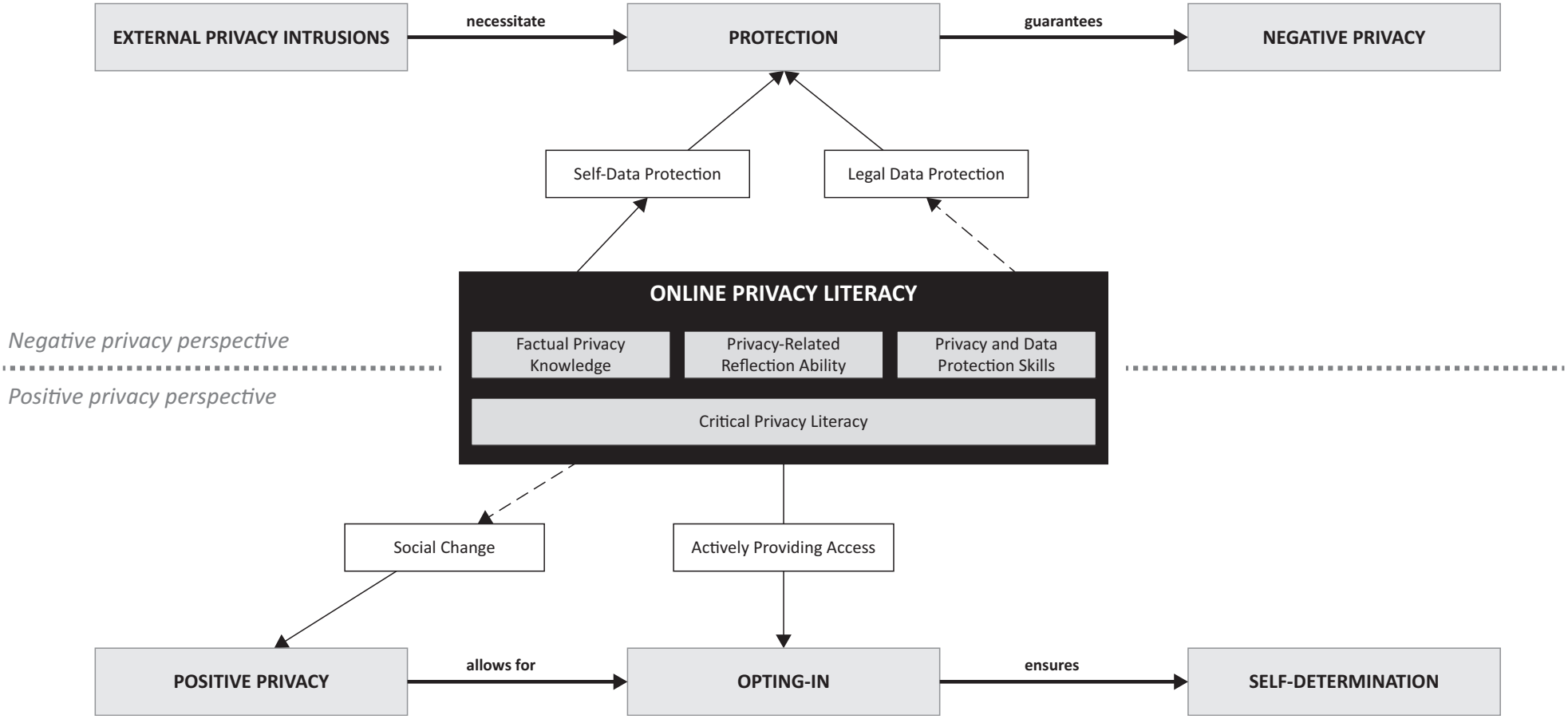

Figure 2. How online privacy literacy supports privacy protection (negative perspective) and informational self-determination (positive perspective). Notes: The dotted arrows represent indirect influences via democratic processes (e.g., changing data protection laws and regulations is only possible via policy making. Individuals can thus only vote for politicians that represent their wishes in the policy making process). Continuous arrows represent direct influences (e.g., with appropriate factual knowledge and data protection skills, individuals can protect themselves and thus ensure protection against external privacy intrusion to guarantee negative privacy).

that provides individuals with "power over their culture and thus enables [them] to create their own meanings and identities to shape and transform the material and social conditions of their culture and society" (Kellner & Share, 2007, p. 18). In a similar way, online privacy literacy may enable individuals to influence the ways in which privacy is defined and handled in their culture and society (Figure 2, lower panel). If individuals gain the ability to identify, challenge, and criticize norms, processes, and social structures that affect the privacy of individuals, they can distance themselves from their own privacy needs, reflect and challenge their entanglement in social relations and power structures, and focus on the greater value of privacy as a collective good.

The fundamental goal then becomes the enforcement and creation of societal conditions that enable informational self-determination and thereby adapt a positive notion of privacy. Under such conditions, the individual no longer needs protection to achieve negative privacy because positive privacy is the default. Instead, individuals voluntarily provide access to themselves whenever they feel it is appropriate. For these decisions, however, online privacy literacy is still needed.

These ideal conditions could be reached by supporting policies that focus on decommodifying user-data and information (Fuchs, 2011; Sevignani, 2016). Politically realizable and previously proposed solutions include more political and economic support for non-commercial internet services that refrain from data collection and are not built upon advertisement-based business models (e.g., Wikipedia; cf. Sevignani, 2013), stronger support of platforms or products that implement 'privacy-by-default' or 'privacy-by-design' (Cavoukian, 2009) and thereby provide users with full agency and control of how their information is used, and implementation of strict forms of the informed consent model (Custers, Hof, & Schermer, 2014). On the institutional level, an even stronger commitment to the right to be forgotten (Rosen, 2012) could further support true informational self-determination. Although such a right has been implemented in the new European Data Protection Regulation (European Parliament, 2017, Art. 7), only few countries so far have applied it in constitutional court decisions (e.g., in Germany, see Friedl, 2019).

If online communication and media use is less governed by information exploitation, provides users with 'opt-in' instead of 'opt-out' (or 'no choice at all') policies, and gives individuals a chance to participate in design and development of communication environments (Ochs & Lamla, 2017; Trepte, 2015), a positive notion of privacy becomes imaginable. Particularly critical online privacy literacy should produce responsible and politically mature citizens that do not only focus on protecting themselves, but question the necessity for protection in general. This shift in perspective should correlate to an increased motivation to participate in democratic processes that may influence the handling and perspective on privacy in the society as a whole. Political engagement in this regard may take several forms from active agenda setting, protests for data protection and privacy rights, participating in the political discourse, engagement in political parties, or voting for parties that support a stronger commitment to informational self-determination.

To date, there is no research on the connection between critical privacy literacy and civic engagement. However, it has been shown that higher media literacy is positively related to political engagement (cf. Alvermann & Hagood, 2000; Mihailidis & Thevenin, 2013). For example, based on a survey of 400 American students, Martens and Hobbs (2015) found that specifically a higher ability to critically analyze news messages—a type of critical thinking ability related to media messages—positively predicted intentions to engage in various civic engagement activities, such as voting in national elections or join a political party. As critical media literacy allows citizens to "gather accurate, relevant information about their society and to question authority" (Mihailidis & Thevenin, 2013, p. 1614) and become "subjects in the process of deconstructing injustices, expressing their own voices, and struggling to create a better society" (Kellner & Share, 2007, p. 20), critical online privacy literacy may likewise allow individuals to use their knowledge about privacy-related aspects of social society to deconstruct the imbalance between powerful economic players, governmental institutions, and weak individual users and thereby become agents of social change. Through increased civic engagement, a social transformation towards a more positive notion of privacy may become possible.

4. Conclusion and Future Perspectives

In this article, I have argued that privacy is predominantly conceptualized in the liberal tradition and in particular as a form of negative freedom. This conceptualization leads to a strong emphasis on privacy protection both in societal debates and academic research. As a consequence, policy making as well as research primarily focus on finding ways to protect the individual against horizontal (i.e., threats stemming from other users) and vertical (i.e., economic or institutional intrusions through data collection and surveillance practices). Although this is important in its own right—as protection against identification and unwanted access to the self or personal information is vital not only in democratic societies, such a perspective fails to question and challenge the circumstances that have led to the necessity for such protection in the first place. I have argued that trying to protect individuals against external influences is similar to treating only the symptoms of a disease instead of its underlying causes. If privacy is conceptualized as a form of positive freedom instead (e.g., as a form of informational self-determination), we can start to ask how societal conditions would need to look like in order to reach such an ideal.

I aimed to show that online privacy literacy paradoxically can be both a means to empower individuals to

protect themselves *and* the fundamental driving force in motivating civic engagement and thus societal change towards establishing informational self-determination. I proposed and refined a model of online privacy literacy that consists of four, interrelated dimensions: 1) factual knowledge about social, economic, institutional, technical, and legal aspects of privacy and data protection, 2) ability to reflect the risks associated with one's own behavior, 3) privacy and data protection skills, and 4) ability to critically evaluate the processes, social structures, and norms that affect the privacy of all individuals and motivation to become agents of social change. Such a combination of knowledge, skills, and abilities provides individuals with the means to engage in self-data protection strategies as well as the awareness of how data protection can be enforced through existing data protection law. At the same time, however, higher online privacy literacy allows individuals to distance themselves from their own privacy needs, reflect and challenge their entanglement in social relations and power structures, criticize the societal conditions that have led to the necessity of privacy and data protection, and focus on the greater value of privacy as a collective good. Online privacy literacy, especially critical privacy literacy, becomes the fundamental requirement for the diffusion of democratic potentials aimed at exploring and supporting ways to decommodify information. It is important to note, however, that such a deliberative process may face considerably challenges in non-democratic societies. In authoritarian regimes in which freedom of speech is not guaranteed, it may not be possible to challenge the status quo and enforce changes through elections, protests, or other types of civic engagement. Given that such actions can be risky for the individual, true informational self-determination may be much harder to demand in non-democratic societies.

Although the outlined processes could be criticized for being too idealistic and external threats (e.g., resulting from economic interests and mass surveillance) cannot be entirely eradicated, we may nonetheless ask how online privacy literacy and particularly critical privacy literacy could be increased on the societal level. One way could be to integrate respective education into existing school curricula. In doing so, online privacy literacy should be taught holistically. Knowledge about economic models of the information society, data collection and surveillance practices, as well as horizontal dynamics of online environments should be imparted in various subjects (e.g., history, political or social sciences). Technical aspects may be taught in computer courses or media education classes. The various knowledge dimensions of online privacy literacy may be taught using traditional didactic learning techniques, but experiential learning (Jacobson & Ruddy, 2004; Kolb, 2014) is a much more promising route to develop critical thinking and reflection abilities as well as to foster digital citizenship. This concept has recently been implemented in educational learning platforms (e.g., Social Media TestDrive; DiFranzo et al., 2019) that focusing not only on teaching hands-on skills through experiences, but prompt young adolescents to reflect and critically engage with online media messages and behaviors.

More importantly, however, this article proposes several avenues for future research on online privacy: First and foremost, privacy scholars should critically investigate whether normative premises as well as practical implications of their research suffer from a too narrow adoption of a negative perspective on privacy. Many articles in the social sciences that investigated privacy and self-disclosure processes in online environments argue that individuals lack the knowledge and skills to protect themselves online (e.g., Hoffmann et al., 2016; Hoofnagle et al., 2010; Masur et al., 2017; Park, 2013; Trepte et al., 2015). As a consequence, scholars often propose privacy literacy education as a potential solution to current privacy problems. However, we should critically evaluate if such a strong focus on trying to find ways to protect individuals' privacy supports a privacy-invasive status quo and hinders scientific analysis of the circumstances that have led to the necessity of protection.

Second, future research should investigate the concept of online privacy literacy in more detail, identify potential subdimensions, develop measurement instruments, and investigate what type of education programs and interventions could foster online privacy literacy. At the moment, most existing scales capture only factual knowledge dimensions (e.g., OPLIS; Masur et al., 2017). Future research should hence develop scales or tests that additionally capture reflection abilities, demonstrate users' procedural knowledge and skills to implement data protection strategies, and objectively test their critical evaluation abilities. Existing approaches to measure media literacy and specifically critical media literacy (e.g., Arke & Primack, 2011; Hobbs & Frost, 2011) may prove useful in developing such tests.

Finally, I argued that higher critical privacy literacy leads to higher willingness to participate in democratic processes. This preliminary hypothesis requires careful empirical investigation. Although one could think of correlating results from a critical privacy literacy test with various measures of civic engagement (e.g., intention to demonstrate for privacy-related purposes or intention to vote for parties that advocate for informational self-determination) using traditional survey designs, I strongly urge future research to develop alternative ways to test this hypothesis. We need ways to test people's online privacy literacy over longer periods of time and observe their demonstration of privacy-related skills in natural environments. Only by investigating the situational context (cf. Masur, 2018b) under which such skills are performed, we may understand how situationally activated goals and cues outplay risk perceptions or critical evaluations of the privacy-invasive nature of an online environment.

Furthermore, theoretical models that aim to explain the role of online privacy literacy should take

well-researched concepts such as online privacy concerns (e.g., Baruh et al., 2017), privacy self-efficacy (e.g., Dienlin & Metzger, 2016), or privacy cynicism (Choi et al., 2018; Hoffmann et al., 2016), but also uncertainty with regard to vertical privacy risks (Acquisti et al., 2015) into account and investigate their entanglement with online privacy literacy in explaining individuals' behavior.

In sum, it seems likely that online privacy literacy plays an important role in addressing the social, economic, and institutional dynamics from which current threats to individuals' privacy emerge. In contrast to predominant assumptions about its potential, however, it may not only empower individual to protect themselves against unwanted identification or access, but also provide individuals with the ability to challenge current societal conditions and explore avenues of societal change towards more positive notions of privacy. Exploring these potentials while taking the proposed model of online privacy literacy into account could provide more meaningful alternatives for achieving informational self-determination on a societal level.

Conflict of Interests

The author declares no conflict of interests.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing.

Alvermann, D. E., & Hagood, M. C. (2000). Critical media literacy: Research, theory, and practice in 'new times.' *The Journal of Educational Research*, *93*(3), 193–205.

Arke, E. T., & Primack, B. A. (2011). Quantifying media literacy: Development, reliability, and validity of a new measure. *Educational Media International*, *46*(1), 53–65.

Baacke, D. (1996). Medienkompetenz: Begrifflichkeit und sozialer Wandel [Media literacy: Concept and social change]. In A. von Rein (Ed.), *Medienkompetenz als Schlüsselbegriff* [Media literacy as a key concept](pp. 112–124). Bad Heilbrunn: Klinkhardt.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior: A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579–596. https://doi.org/10.1177/1461444815614001

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Berlin, I. (1969). *Four essays on liberty*. Oxford: Oxford University Press.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles.* Toronto: Information and Privacy Commissioner of Ontario. Retrieved from https://www.ipc.on.ca/wpcontent/uploads/Resources/7foundationalprinciples.pdf

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Custers, B., Hof, S. v. d., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy & Internet*, *6*(3), 268–295. https://doi.org/10.1002/1944-2866.POI366

Dienlin, T., & Metzger, M. J. (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*, 368–383. https://doi.org/10.1111/jcc4.12163

DiFranzo, D., Choi, Y. H., Purington, A., Taft, J. G., Whitlock, J., & Bazarova, N. N. (2019). Social media test-drive: Real-world social media education for the next generation. In S. Brewster, G. Fitzpatrick, A. Cox, & V. Kostakos (Eds.), *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1–11). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3290605.3300533

European Parliament. (2017). *The European general data protection regulation*. Brussels: European Parliament. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Friedl, P. (2019, December 12). New laws of forgetting: The German Constitutional Court on the right to be forgotten. *European Law Blog.* Retrieved from https://europeanlawblog.eu/2019/12/12/new-laws-of-forgetting-the-german-constitutional-court-on-the-right-to-be-forgotten

Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4), 220–237. https://doi.org/10.1108/14779961111191039

Fuchs, C. (2012). The political economy of privacy on Facebook. *Television & New Media*, *13*(2), 139–159. https://doi.org/10.1177/1527476411415699

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*(3), 421–471.

German Constitution. art 1, §1.
German Constitution. art. 2, §1.
Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the surveillance state*. New York, NY: Hamish Hamilton.
Groeben, N. (2002). Dimensionen der Medienkompetenz: Deskriptive und normative Aspekte [Dimensions of media literacy: Descriptive and normative aspects]. In N. Groeben & B. Hurrelmann (Eds.), *Medienkompetenz: Voraussetzungen, Dimensionen, Funktionen* [Media literacy: Requirements, dimensions, functions] (pp. 160–197). Weinheim: Juventa.
Gutwirth, S., Leenes, R., & de Hert, P. (Eds.). (2015). *Reforming European data protection law* (Vol. 20). Dordrecht: Springer.
Gutwirth, S., Leenes, R., & de Hert, P. (Eds.). (2016). *Data protection on the move: Current developments in ICT and privacy/data protection* (Vol. 24). Dordrecht: Springer.
Hobbes, T. (1651). *Leviathan*. Seattle, WA: Pacific Publishing Studio.
Hobbs, R., & Frost, R. (2011). Measuring the acquisition of media-literacy skills. *Reading Research Quarterly*, *38*(3), 330–355.
Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7
Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1589864
Horvát, E.-Á., Hanselmann, M., Hamprecht, F. A., & Zweig, K. A. (2012). One plus one makes three (for social networks). *PLoS ONE*, *7*(4). https://doi.org/10.1371/annotation/c2a07195-0843-4d98-a220-b1c5b77a7e1a
Jacobson, M., & Ruddy, M. (2004). *Open to outcome: A practical guide for facilitating and teaching experiential reflection*. Oklahoma City, OK: Wood N. Barnes.
Kellner, D., & Share, J. (2007). Critical media literacy, democracy, and the reconstruction of education. In D. Macedo & S. R. Steinberg (Eds.), *Media literacy: A reader* (pp. 3–23). New York, NY: Peter Lang.
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002
Kolb, D. A. (2014). *Experiential Learning: Experience as the source of learning and development* (2nd ed.). Upper Saddle River, NJ: Pearson FT Press.
Kraus, L., Wechsung, I., & Möller, S. (2014). *A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior*. Paper presented at the Workshop on Privacy Personas and Segmentation (PPS) at the Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA, USA.
Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, *7*(1), 3–14. https://doi.org/10.1080/10714420490280152
Martens, H., & Hobbs, R. (2015). How media literacy supports civic engagement in a digital age. *Atlantic Journal of Communication*, *23*(2), 120–137. https://doi.org/10.1080/15456870.2014.961636
Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313
Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995
Masur, P. K. (2018a). Mehr als Bewusstsein für Privatheitsrisiken. Eine Rekonzeptualisierung der Online: Privatheitskompetenz als Kombination aus Wissen, Fähig und Fertigkeiten [More than risk awarness: A reconceptualization of online privacy literacy as a combination of knowledge, abilities, and skills]. *Medien & Kommunikationswissenschaft*, *66*(4), 446–465. https://doi.org/10.5771/1615-634X-2018-4-446
Masur, P. K. (2018b). *Situational privacy and self-disclosure: Communication processes in online environments*. Cham: Springer.
Masur, P. K., Teutsch, D., Dienlin, T., & Trepte, S. (2017). Online-Privatheitskompetenz und deren Bedeutung für demokratische Gesellschaften [Online privacy literacy and its role in democratic societies]. *Forschungsjournal Soziale Bewegungen*, *30*(2), 180–189.
Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS) [Development and validation of the online privacy literacy scale (OPLIS)]. *Diagnostica*, *63*(4), 256–268. https://doi.org/10.1026/0012-1924/a000179
Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data." *Journal of Information, Communication and Ethics in Society*, *12*(2), 93–106. https://doi.org/10.1108/JICES-08-2013-0030
Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection: Empowerment or burden? In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Data protection on the move* (pp. 277–305). Cham: Springer.
Mihailidis, P., & Thevenin, B. (2013). Media literacy as a core competency for engaged citizenship in participatory democracy. *American Behavioral Scientist*, *57*(11), 1611–1622. https://doi.org/10.1177/

0002764213489015
Mill, J. S. (2015). *On liberty*. Middleton: CreateSpace. (Original work published 1859)
Miller, A. R. (1971). *The assault on privacy: Computers, data banks, and dossiers*. Ann Arbor, MI: University of Michigan Press.
Moore, B. (1984). *Privacy: Studies in social and cultural history*. New York, NY: Pantheon Books.
Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford Law Books.
Ochs, C., & Lamla, J. (2017). Demokratische Privacy by Design [Democratic privacy by design]. *Forschungsjournal Soziale Bewegungen*, *30*(2), 189–199. https://doi.org/10.1515/fjsb-2017-0040
Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338
Petronio, S. (2002). *Boundaries of privacy*. Albany, NY: State University of New York Press.
Potter, W. J. (2008). *Media literacy* (4th ed.). Los Angeles, CA: Sage.
Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, *4*(4), 323–333.
Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First *Monday*, *15*(1). https://doi.org/10.5210/fm.v15i1.2775
Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online*, *64*, 88–92.
Sarigol, E., Garcia, D., & Schweitzer, F. (2014). Online privacy as a collective phenomenon. In A. Sala, A. Goel, & K. Gummadi (Eds.), *Proceedings of the Second ACM conference on online social networks* (pp. 95–106). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/2660460.2660470
Seubert, S., & Becker, C. (2019). The culture industry revisited: Sociophilosophical reflections on 'privacy' in the digital age. *Philosophy & Social Criticism*, *45*(8), 930–947. https://doi.org/10.1177/0191453719849719
Sevignani, S. (2013). The commodification of privacy on the Internet. *Science and Public Policy*, *40*(6), 733–739. https://doi.org/10.1093/scipol/sct082
Sevignani, S. (2016). *Privacy and capitalism in the age of social media*. New York, NY: Routledge.
Solove, D. J., & Schwartz, P. M. (2019). *Privacy law fundamentals.* Portsmouth, NH: International Association of Privacy Professionals.
Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology*, *18*(1), 33–39. https://doi.org/10.1007/s10676-016-9392-2
Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x
The Economist Intelligence Unit. (2020). *Democracy index 2019: A year of democratic setbacks and popular protest*. London: The Economist Intelligence Unit.
TOR. (2020). The Onion Router. Retrieved from https://www.torproject.org
Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media + Society*, *1*(1), 1–2. https://doi.org/10.1177/2056305115578681
Trepte, S., & Masur, P. K. (2017). The need for privacy. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of personality and individual differences*. (pp. 1–4). London: Springer.
Trepte, S., & Reinecke, L. (2011). The social web as shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 61–74). Berlin: Springer.
Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Dordrecht: Springer.
Turow, J. (2003). *Americans online privacy: The system is broken* (Report 6-2003). Philadelphia, PA: The Annenberg Public Policy Center of the University of Pennsylvania.
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.
Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.
Wolf, R. d., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, *35*, 444–454. https://doi.org/10.1016/j.chb.2014.03
Zuboff, S. (2019). *The age of surveillance capitalism*. New York, NY: Public Affairs.

About the Author

Philipp K. Masur is a Postdoctoral Research Associate at the Department of Communication at Johannes Gutenberg University Mainz (Germany). He earned his PhD from the University of Hohenheim (Stuttgart, Germany) in 2018. His research focuses on privacy and self-disclosure processes in online environments, social norms in networked public, communication and well-being, and empirical research methods.