Challenges in studying social media privacy literacy

Masur, Philipp K.; Hagendorff, Thilo; Trepte, Sabine

published in
The Routledge Handbook of Privacy and Social Media
2023

DOI (link to publisher)
10.4324/9781003244677-13

document version
Publisher's PDF, also known as Version of record

11

CHALLENGES IN STUDYING SOCIAL MEDIA PRIVACY LITERACY

Philipp K. Masur[1], *Thilo Hagendorff*[2], *and Sabine Trepte*[3]

[1]VRIJE UNIVERSITEIT AMSTERDAM, THE NETHERLANDS
[2]UNIVERSITY OF TUEBINGEN, GERMANY
[3]UNIVERSITY OF HOHENHEIM, GERMANY

Introduction

In any discussion about online privacy, people will put forth that we would simply need to foster sufficient privacy literacy among Internet users to ensure an appropriate level of protection and self-determination. Almost like a mantra, future perspectives in privacy-related academic articles recommend increasing privacy-related awareness, knowledge, and skills to address whatever privacy threat they outlined. It almost seems that sufficiently high online privacy literacy would be the ultimate solution, promising to solve all problems – from preventing privacy violations by other users to countering the power imbalance between users and providers of privacy-invasive technologies. Therefore, it is perhaps no surprise that the previously termed "knowledge gap hypothesis," that Internet users simply lack the knowledge and skills to protect their privacy (Trepte et al., 2015), can be found in almost every area of privacy research. Many chapters in this volume support this notion. For example, it "solves" the privacy paradox by suggesting that people's concerns do not translate into privacy protection behavior because they simply do not know how to do so. It respectively "explains" the emergence of privacy cynicism because unawareness of data and privacy protection strategies or alternative, privacy-friendly services seems to give rise to the feeling that any attempt to protect one's privacy is futile (see chapter 13 by Ranzini et al. on privacy cynicism). It likewise "provides" an explanation for why people value benefits over risks in disclosure decision processes (see chapter 7 by Dienlin on the privacy calculus) or fall prone to misleading heuristics and biases (see chapter 8 by Liao et al. on heuristics and privacy). In fact, a common recommendation by academics and policy makers is to make people more literate. After all, investing in education never sounds wrong politically. Yet, as we will discuss later, the immediate appeal of educating the people shifts the responsibility to the individual who may thereby have to deal with a considerable burden, rather than experience true empowerment.

In this chapter, we focus on *social media* privacy literacy specifically as the question of whether people lack knowledge and skills to protect their privacy is particularly often posed in the context of social media. And indeed, successfully managing different information contexts and identities on such platforms without causing a "context collapse" (Nissenbaum, 2010; Vitak, 2012) has become quite difficult. To control personal information, audiences, and communications channels in

 DOI: 10.4324/9781003244677-13

accordance with one's privacy needs requires deep familiarity with the architecture and settings of the respective social media platform, but also how information flows both horizontally (between users) and vertically (between users and platform providers; Bazarova & Masur, 2020). Privacy turbulence resulting from a lack of social media privacy literacy particularly can result in feelings of embarrassment, trouble at work or school, relationship problems, etc. Hence, the ability to self-monitor one's online behavior has become increasingly important for social media users.

We believe that the study of (social media) privacy literacy is worthwhile if not pivotal to advance privacy and social media research at this point in time. But we also acknowledge that fostering privacy literacy is only one aspect of a necessarily multi-layered response to the increasing privacy threats that must be concerted with legal regulation and data protection (Hagendorff, 2018). In this chapter, we provide an overview of the conceptual, theoretical, and empirical frameworks of online privacy literacy and how it is applied to the context of social media. We discuss their strengths and weaknesses, review empirical evidence for the knowledge gap hypothesis, and outline the potential of educational interventions to foster social media privacy literacy. We close with what we consider the most pressing avenues for future research.

From Online Privacy Literacy to Social Media Privacy Literacy

Any type of literacy can be traced back to the 1970s, during which the term "literacy" (sometimes also "competence"), first introduced in linguistics, was established and applied to developmental and social theories (Sutter & Charlton, 2002). Chomsky (1976) originally differentiated competence (knowledge about a language and its rules) from performance (the actual use of language in concrete situations) and thereby started a long and on-going tradition of investigating literacies. Being *literate* means having the necessary knowledge, abilities, and skills as well as the motivational, volitional, and social willingness to solve certain problems (cf. Weinert, 2003). Such a broad definition implies that for every problem (from all-encompassing to microscopic specific), we could technically define a respective set of knowledge, skills, and abilities, which could (and in part has led) to a conceptual jungle. For the ability to speak a language, it may be possible to clearly identify the relevant rules that need to be known (although even this is disputed). With regard to privacy literacy, one cannot help but feel a little uneasy that anything from abstract meta-competencies such as "being able to think critically" to concrete and specific skills such as "being able to limit access to the self by setting the visibility of Facebook posts to only close friends" could be justified as a valid dimension.

What exactly encompasses online privacy literacy thus becomes a normative question. Any proposal for an online privacy literacy model takes a stance on what *should* be known and what abilities *should* be possessed (cf. Groeben, 2002). Relevant knowledge, abilities, and skills are thereby often motivated by their proposed potential to lead to a certain behavior (e.g., more data protection, less disclosure, more use of privacy settings …). From our point of view, both abstract definitions that outline important meta-competencies (e.g., "being able to critically reflect") as well as more specific definitions that outline the respective sets of knowledge, skills, and abilities for certain target groups, platforms, services, and contexts (e.g., "ability to use Facebook friend's lists feature to limit access to posts") have merit and help to gain a deeper understanding of privacy literacy overall.

Online Privacy Literacy

In light of this, online (and, in turn, social media) privacy literacy must be seen within the tradition of media literacy and computer literacy concepts that originated as a response to the increasing mediatization and digitalization of society. Early media literacy concepts mostly embodied a so-called

protectionist approach and focussed on expanding awareness of risks and providing means and ways to protect oneself against potentially negative outcomes of media use (cf. Potter, 2010). Early online privacy literacy research similarly was a response to emerging risks of privacy violations in the context of digital technologies. The first studies hence investigated relationships between awareness of privacy-invasive practices by online service providers as well as knowledge about technical aspects of data protection and the implementation of actual data protection behavior (e.g., Hoofnagle et al., 2010, Park, 2013, Turow, 2003). With regard to its technical dimension, privacy literacy is thereby akin to computer literacy, comprising mostly the knowledge to understand and the abilities to appropriately control user interfaces to manage privacy.

Yet, as media scholars stressed the balance between protection and empowerment in conceptualizing media literacy (e.g., Baacke, 1996, Groeben, 2002b; Hobbs, 2010), privacy scholars similarly reframed privacy literacy to encompass users' ability to not just protect themselves, but also actively and meaningfully use online services in alignment with their privacy needs. Trepte et al. (2015) expanded original models by distinguishing factual knowledge about technical, economic, and legal aspects of privacy and data protection from procedural knowledge about how to implement data protection strategies.

Building on this multi-dimensional model, Masur (2020) provided an Extended Model of Online Privacy Literacy that includes a) factual privacy knowledge, b) privacy-related reflection abilities, c) privacy and data protection skills, and d) critical privacy literacy. This broader conceptualization acknowledges that users need knowledge and awareness about data collection practices, data protection regulations, technical aspects related to information flow as well as awareness of horizontal privacy dynamics on different online platforms, but further highlights the need for abilities and skills that translate this abstract knowledge into actual behavior that reflects their individual needs. Next to factual knowledge, it first proposes privacy-related reflection abilities that allow users to identify specific risks (in Altman's (1975) terms: Assessing the actual level of privacy) in different online environments and assess them in light of their own individual privacy needs (Altman: Comparing the actual with their desired level of privacy). Based on this constant comparison, people then, secondly, should be able to reflect on whether their behavior contributes to such a misbalance.

Based on risk awareness and reflection, users thirdly need specific skills to manage information flows. Information management, then, can be applied in several ways. It comprises data parsimony, using encryption techniques, cutting interconnections between computers, digital rights managements, using firewalls, password prompts, and the like. These measures can take place at the front- or backend of digital platforms and services. Ultimately, privacy protection strategies also include choosing more privacy-friendly platforms over privacy-intrusive ones.

Whereas the previous three dimensions shall empower users to learn and possess a range of competencies and abilities to use and share personal information in a way that protects their privacy against horizontal or vertical intrusions, a fourth dimension proposed by Masur (2020), called critical privacy literacy, acknowledges that self-data protection against some vertical privacy intrusions may be futile. In fact, despite sufficient knowledge about privacy-invasive practices, the reflection of one's behavior, and skills to protect one's privacy, the means to actually minimize the power of online service providers to harness an individual's data is severely limited. Critical privacy literacy refers to the "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" (Masur, 2020, p. 261). Such a type of literacy, which was already introduced to broader concepts of media literacy concepts some decades ago (e.g., Baacke, 1996; Groeben, 2002b), can thus be regarded as a fundamental requirement for actualizing the democratic potential of individuals to shape and transform the social conditions of their society (cf. similarly expressed for critical media literacy by Kellner & Share, 2005).

Social Media Privacy Literacy

Social media privacy literacy is best understood as online privacy literacy applied to the specific context of social media. To our knowledge, most studies that investigate privacy literacy in the context of social media do not explicitly define social media privacy literacy. Instead, drawing from the extended literature on online privacy literacy as discussed above, they apply relevant competencies from existing online privacy literacy models to the context of social media (e.g., Bartsch & Dienlin, 2016; Choi, 2022). This application process can be understood by looking at items that these scholars used to assess social media-specific privacy literacy. For example, Bartsch and Dienlin (2016) used items such as "I know how to restrict access to my postings." Choi 2022) similarly employed items such as "I have the knowledge necessary to use privacy features to regulate information on Facebook." Such operationalizations are akin to the procedural skills dimensions included by Trepte et al. (2015) or Masur (2020), but apply them specifically to the privacy settings available on Facebook. Unfortunately, studies in this area hardly focus on other than the procedural skill dimensions of overall privacy literacy.

That said, there is also growing literature on social media literacy (basically the more general concept of media literacy applied to the context of social media), which often acknowledges privacy as a particular domain relevant to successfully navigating and using such platforms (e.g., Livingstone, 2014; Purington et al., 2022). Here, we again see scholars defining core competencies of (social media) media literacy (e.g., access, evaluate, reflect, generate …) as an umbrella that, in turn, is applied to specific domains (such as, e.g., privacy, advertising, news, phishing, …). For example, Purington et al. (2022) define social media literacy as "the ability to 1) find and access social media platforms and use them and their respective options and channels skillfully, 2) critically evaluate social media content and its potential consequences, 3) generate creative social media content with an awareness of the specific audience, 4) reflect on one's own behavior, apply social responsibility, and adequately manage one's affective responses, and 5) develop and perpetuate prosocial behavioral norms and exhibit digital citizenship" (p. 6). The authors then argue that although meaningful in getting an understanding of what social media literacy entails, these five meta-competencies need to be applied to different domains (including privacy) to make them amenable to empirical investigation. For example, in their scale development process, they narrow these rather abstract dimensions down to specific social media use situations, in which privacy may be threatened or negotiated.

As outlined earlier, media literacy concepts have long included the notion that it should empower users and help them serve their needs. Whereas protection clearly addresses the question of "protection *from* what?", empowerment refers to the question "empowerment *for* what?". Whereas the first question could be deemed sufficiently answered in previous research, we would like to add some reflections on the latter. Inspired by Groeben's (2002b), we suggest that literacy also caters to the experiences of positive media uses and effects. Social media privacy literacy thus would mean that users choose privacy settings and manage their connections and content in a way that it empowers them for enjoyment and other more fundamental needs. Privacy, in fact, can be seen as a condition that serves the fulfillment of fundamental needs (Masur, 2018). Pedersen (1997), for example, proposed rejuvenation, contemplation, and creativity as psychological functions of privacy. Taken together with Groeben's idea on literacy, we conclude that social media literacy also refers to the ability to create private (or at least contextually appropriately protected) spaces that empower users for rejuvenation, contemplation, enjoyment, and creativity. Under the cloak of anonymity, users may be empowered for rejuvenation by reading and browsing through content they like without fearing repercussion. Protected against vertical intrusions, they may be empowered for contemplation by dreaming themselves into the world of fantasy catered by other users and storytellers. Or in some online spaces (such as friend groups, or public spaces that rely on pseudonyms), they may creatively try out new activities or identities. In sum, social media privacy literacy also means finding the right balance

between withdrawal and participation to find the appropriate level of access that still allows one to benefit from the many offers that social media offers.

We believe that the manifold approaches to conceptualizing online privacy literacy and social media privacy literacy, respectively, are a testament to a vibrant research community. Reconciling different definitions and concepts may be a noble endeavor, but ultimately will fail as an all-encompassing concept will necessarily always be too abstract to inform concrete intervention (see chapter 1 in this handbook on defining privacy by Trepte and Masur). A platform- or even context-specific concept, in contrast, may always be too specific to allow for generalizations beyond their specifically outlined circumstances. With that said, we want to contribute to the literature by offering dynamic definition of social media privacy literacy that is based on the research discussed above (particularly, Masur, 2020, Park, 2013; Trepte et al., 2015). We thereby acknowledge that such a literacy has to take both vertical (information flow between users and the provider) and horizontal (information flow between users) privacy issues into account.

From this point of view, social media privacy literacy can be grasped by four meta-competencies that further include several subdimensions.

1 Factual knowledge (a) on a vertical level about economic interests and data collection, analysis, and sharing practices of social media providers and (b) on a horizontal level about information flow, communication practices, and social dynamics between users of the social media platform.
2 Privacy-related reflection ability includes (a) the ability to identify privacy risks, turbulence, and violations during social media use, (b) the ability to reflect one's privacy needs in such situations, and (c) the ability to evaluate one's own posting and communication behavior as well as (d) use of privacy-preserving strategies to create an appropriate balance between protection and empowerment, or, in other words, need satisfaction and risks. Privacy is not an end by itself, but only meaningful when it allows for more fundamental needs such as intimacy with other close people, relationship building, enjoyment, creativity, etc.
3 Procedural skills that include (a) the ability to evaluate social media platforms and, if necessary, choose more privacy-friendly alternatives, (b) knowledge about how to implement platform-specific privacy strategies and how to use their proprietary privacy settings, (c) the ability to monitor disclosure according to one's need (data parsimony), but also (d) the ability to use all of these skills in a contextually appropriate way that not only secludes them from social interaction, but rather creates spaces for sociality, connection, rejuvenation, contemplation, creativity, and overall enjoyment.
4 Critical privacy literacy includes the ability to question and criticize communication practices, social dynamics, the socio-technological architecture of social media, and both vertical and horizontal information flows that affect individuals' privacy and their ability to use social media in ways that benefit and empower them.

Depending on the type of research question, not all competencies and subdimensions may be equally important to assess. We nonetheless hope that this broad definition will provide nuance to the study of privacy in the context of social media. Yet, even if we settle on such a working definition, how can we empirically measure social media privacy literacy?

How to Measure Social Media Privacy Literacy?

Being able to (objectively) measure a person's social media privacy literacy is crucial for several reasons: First, it is needed to determine individuals' familiarity with privacy issues, assess general knowledge gaps, and evaluate the overall severity of missing literacy in a population. Second, it allows us to put the knowledge gap hypothesis under empirical scrutiny. Only by gaining a good

understanding of people's literacy levels, we can investigate antecedents and outcomes and better understand the role of knowledge and skills in shaping users' online behavior. And finally, only by assessing literacy as an outcome, we can evaluate potential educational interventions.

Yet, measuring literacy is easier said than done. Whereas some dimensions of literacy such as *knowledge* may be assessed through traditional test formats, others such as *reflection abilities* can only be demonstrated and thus observed. This refers to a common problem of literacy in general: Instead of literacy itself, we can only observe the performance of literate behavior, from which we then conclude certain literacies (cf. Sutter & Charlton, 2002). It is thus perhaps hardly surprising that the measurement of online privacy literacy is often based on self-reports and thus remains entirely subjective and potentially biased (e.g., Choi, 2022; Masur, 2018). In an attempt to make the measurement of online privacy literacy more objective, some scholars created knowledge tests that consist of several true–false statements (e.g., Hoofnagle et al., 2010; Park, 2013). In such tests, participants read several statements (e.g., "Companies today have the ability to place an online advertisement that targets you based on information collected on your web-browsing behavior" – TRUE; Park, 2013) and had to decide whether it was true or false. Correct answers are then summed up as an index of literacy.

For their multi-dimensional model of privacy literacy, Masur and colleagues (Masur et al., 2017; Trepte et al., 2015) developed the online privacy literacy scale (OPLIS), which represents a comprehensive questionnaire to objectively assess factual and procedural knowledge in relation to online privacy and data protection. It represents a knowledge test that was validated in several studies and consists of 20 multiple-choice and true–false items (five per dimension) that assess people's knowledge about institutional practices, technical aspects, legal aspects, and data protection strategies (example item: "Companies combine users' data traces collected from different websites to create user profiles" – TRUE).[1] The final scale allows for investigating both individual dimensions as well as overall online privacy literacy and has since been used in several empirical studies.

Social media privacy literacy seems to be mostly assessed with short scales. Bartsch and Dienlin (2016), for example, used six self-report items (e.g., "I know how to delete or deactivate my account"). Cho (2022) used two similar items (e.g., "I have the knowledge necessary to use privacy features to regulate information on Facebook"). Purington et al. (2022) developed 15 items to assess social media literacy in the domain of privacy.[2] Their instrument represents an objective knowledge test for youth populations (aged 9–13 years) in which participants have to answer questions in a multiple-choice format (e.g., "Why can it be a problem to share something personal on social media? A: Because things you share on social media can stay there forever (*true answer*), B: Because your parents might find out about it, C: Because social media is not for young people, D: It is not a problem. It is actually a lot of fun!").

In sum, the assessment of online privacy literacy has come a long way, yet only a few comprehensive and validated instruments exist. Furthermore, instruments for less knowledge-based dimensions are lacking. With regard to social media privacy literacy specifically, only a few ad-hoc scales exist that mostly rely on self-reported literacy.

Empirical Findings

Several empirical investigations have provided support for a positive link between online privacy literacy and the implementation of privacy behaviors. For example, based on a survey of 419 US-American Internet users, Park (2013) found that technical familiarity, awareness of institutional practices, and privacy policy understanding positively predicted both social (e.g., avoiding particular platforms, using pseudonyms, rectifying information) and technical protection behaviors (e.g., clearing browser history, using PET software). The effect sizes for these relationships were medium. Masur et al. (2017), based on a representative sample of 1,945 German Internet users, likewise found that higher online privacy literacy (i.e., more correct answers in their 20-item scale) positively

predicted the use of active data protection strategies (e.g., using pseudonyms in emails or during registering for websites, using encryption or PET software …). Yet, higher literacy did not predict passive measures such as not using a certain service. Harborth and Pape (2020) similarly showed that higher literacy positively predicts using the anonymization service TOR while negatively predicting trust in online service providers. Masur (2018) also found that higher subjective privacy literacy positively predicted the use of end-to-end encryption and pseudonymization. Sindermann et al. (2021) provide further evidence for this relationship as they found a moderate positive relationship between online privacy literacy and various online privacy behaviors (including changing passwords, using TOR, not using services, etc.). A meta-analysis by Baruh et al. (2017) found, based on ten studies, that privacy literacy was moderately and positively related to the use of privacy protection measures ($r = .29$). Yet, the same meta-analysis also revealed no relationship between privacy literacy and information sharing ($r = .04$).

With regard to the predictive power of social media privacy literacy in particular, there are mostly cross-sectional survey studies that support a positive relationship between higher literacy and the implementation of privacy strategies on social media. For example, Bartsch and Dienlin (2016) surveyed 640 German Facebook users and found that higher privacy literacy positively predicts whether Facebook users restrict the visibility of information on their profile. Based on 1,572 German Internet users, Masur (2018) found that higher privacy literacy negatively predicted the use of privacy-invasive instant messenger (e.g., WhatsApp) and positively predicted the use of privacy-friendly alternatives (e.g., Threema). Yet, these results were less conclusive with regard to other platforms (e.g., Facebook, Instagram, etc.). In a survey of 689 US-American Internet Users, Epstein and Quinn (2020) found that higher privacy literacy positively predicted the implementation of horizontal strategies, which comprise the use of social media-specific privacy settings such as restricting access to photos, posts, or profile. Based on a survey with 322 participants from the US, Choi (2022) found that higher privacy literacy positively predicted whether social media users felt that they own the information they share on Facebook.

Longitudinal analyses of such relationships are generally rare. That said, Schäwel and colleagues (2021) found, based on a two-wave panel survey of 898 German Internet users, that higher online privacy literacy at T1 was positively related to more engagement in data protection behavior at T2 while controlling for the auto-regressive path of online privacy literacy at T1. Yet, this cross-lagged longitudinal effect was rather small. The between-person correlation at T1, however, aligned with prior research and resulted in a medium positive relationship between online privacy literacy and data protection behavior.

Whereas all of the above-mentioned studies speak for the effectiveness of online and social media privacy literacy in enabling more data protection behavior, explicit empirical tests of the knowledge gap hypothesis are rare. For example, only a few studies have explicitly investigated whether a lack of online privacy literacy could explain the privacy paradox (the often observed discrepancy between privacy concerns and privacy behaviors). Schubert et al. (2022), for example, conducted a study with 207 participants who answered a survey and provided the researchers with access to their Facebook profiles. The results show that privacy concerns and privacy literacy interacted in predicting how much data participants' shared on their profiles. For people with high literacy, the relationship between privacy concerns and data sharing becomes negative, thus not supporting the privacy paradox.

Despite these empirical findings, privacy-literacy-driven self-monitoring has its limits since one must assume that users do on many occasions deviate from rational information management (Spottswood & Hancock, 2017; Trepte et al., 2020). They effectively share personal information, are triggered by system-1 thinking or impulses, are subject to addictive routines that are intentionally fostered by the way social media platforms' user interfaces are designed, and many more (Gambino et al., 2016; see also chapter 8 by Liao, Sundar, and Rosson on online privacy cues and heuristics). Privacy literacy may also be a risk in itself. Users who deem themselves to possess comprehensive

privacy literacy may feel that they have higher degrees of control over their personal information. Hence, they may be tempted to disclose all the more sensitive information compared to individuals who feel less literate and are thus more likely to have increased privacy concerns (Acquisti & Gross, 2006; Brandimarte et al. 2013). Ultimately, the feeling of safety that privacy literacy conveys may lead to a misplaced trust in mechanisms for information control.

In sum, the literature suggests a comparatively robust, positive relationship between online privacy literacy and various privacy protection strategies, both generally (e.g., while using the Internet) and specifically (while using social media). The effect sizes range from small ($r = 0.10$) to medium ($r = 0.20$). Longitudinal studies and experimental designs that could offer more insights into causal mechanisms are rare (for an exemption, see again Schäwel et al., 2021). Furthermore, many studies used either OPLIS or self-report measures to assess online privacy literacy. Studies with more comprehensive measures that also included reflection or critical evaluation skills hardly exist.

Educational Interventions to Foster Social Media Privacy Literacy

Somewhat independent of the academic research on the role of (social media) privacy literacy, there are more and more attempts to foster social media literacy in practical and educational contexts. These programs and resources almost always include modules specifically designed to foster privacy literacy, and often particular with regard to social media use. For example, social media platform providers such as Facebook[3] and Google[4] provide digital resources for educators, parents, or caregivers givers that aim to teach concepts of online privacy, setting use, and data parsimony. The teaching style is often a combination of gamification and quizzes. Educational institutions such as, e.g., common sense education in the United States,[5] Landesmedienanstalten in Germany,[6] federal ministries of education and research,[7] or the Netwerk Mediawijsheid in the Netherlands[8] to name just a few likewise offer lesson plans, educational tools, and resources. Also, profit-oriented social media literacy agencies develop and sell their programs in the form of road shows or apps to schools and other educational institutions. Finally, universities have started to turn to the public and offer courses, e.g., on the identification of fake news or deep fakes. Yet, most of these educational resources are not tested rigorously and their impact on knowledge, skills, and actual behavior remains unclear. An exception is Social Media Testdrive, an interactive learning platform that simulates social media use context for learning purposes and includes various modules that aim to foster privacy literacy on social media (including, e.g., "Accounts and Passwords," "Is It Private Information?", and "Shaping your Digital Footprint").[9]

Other studies suggest that critically engaging with social media, in general, may already foster higher privacy literacy. Higdon (2021) investigated the impact of a semester-long course called "Social Media, Social Change" at a Northern Californian University on social media attitudes and behavior. The course was implementing a critical pedagogy approach, relying on in-depth discussions of papers, news, books, and media content on the topic. Based on a qualitative assessment of participants' privacy concerns before and after the course, the author concluded that the course increased awareness and concerns about data collection practices of social media providers. Similarly, Gruzd et al. (2021) confronted 92 Facebook users with an intervention called "Data Selfie," which allows users to examine the types of algorithmic predictions that can be made from their own Facebook data (e.g., about personality, political orientation, or purchasing habits). They found an increase in privacy concerns after the intervention as well as a higher likelihood of engaging in privacy-protective strategies (such as using fake names or information, expressing dissatisfaction privately and publicly, etc.).

Overall, there is sufficient evidence for the potential of educational interventions, courses, and resources to foster higher (social media) privacy literacy among users. Combined with evidence from meta-analyses testing the effect of media literacy interventions on various outcomes such as knowledge, skills, media use, etc. (e.g., Jeong et al., 2012), it seems fruitful to continue developing such interventions, particularly in order to adapt them to different age groups and audiences. We further suggest stressing social media privacy literacy's aim to empower social media use for the satisfaction of fundamental needs for sociality, creativity, or enjoyment as outlined in all dimensions of our social media privacy literacy dimension. What if interventions and education start by defining what users find most enjoyable about social media? What if they start by acknowledging individuals' needs of rejuvenation, contemplation, and creativity when using social media and then turn to possible privacy risks emanating from social media that could hinder the fulfillment of these needs? We will further elaborate on the balances of individual needs and external support in their fulfillment in the following.

Education or Legislation?

In light of the conceptual challenges and empirical findings discussed above, it is worth asking whether or not we should proceed to invest large amounts of money and effort into online privacy literacy education. As mentioned earlier, we believe in the value of investigating and ultimately fostering privacy literacy, but we see it as only one of several necessary responses to dealing with the challenges surrounding online privacy. A higher social media privacy literacy may without a doubt empower individuals to protect themselves against some privacy turbulences when using social media (particularly against horizontal privacy threats such as unwanted exposure, unwanted dissemination of private information by other users, etc.). Nevertheless, many vertical intrusions by providers of social media platforms can hardly be solved through higher literacy, but need to be addressed as well.

Discourses on privacy literacy sometimes tacitly agree with the fact that individual users are burdened with responsibilities for tasks which could also be seen as part of government duties (Hagendorff, 2018). In short, responsibility may be transferred from the state to single individuals who are in many regards not effectively able to govern IT companies, regulate algorithms, and effectively ensure general privacy standards (Matzner et al., 2016). Even individuals who can be deemed to be perfectly privacy literate have limited opportunities to protect themselves against certain privacy violations. One reason for this lies in corporations' ability to accurately infer very sensitive or intimate personal information from prima facie "unsuspicious" data traces via simple machine learning models. Digital footprints of all kinds can be utilized in order to obtain information about various personality traits, personal states, future behavior, etc., (Binder et al., 2022; Lambiotte et al., 2014; Matz et al., 2019; Schäwel et al., 2021) that are very likely to be so intimate that under normal circumstances, affected individuals would clearly object to disclosing them. Furthermore, machine learning techniques allow for gathering information that results from the interactions of the elements of large datasets, but which in itself is not part of them. This is why individualistic notions of privacy or privacy literacy are complemented by concepts like "predictive privacy" (Mühlhoff, 2021) where researchers stress the collective nature of privacy protection measures. However, it remains wishful thinking to hope for a halt of privacy violations that target single individuals but are based on utilizing data other individuals provide about themselves.

In fact, various measures necessary for effective privacy protection are out of reach for individual users and can only be undertaken by state agencies that are authorized to regulate and limit data collection, processing, and dissemination. Substantial advances in surveillance and data-mining applications create a significant power imbalance between individual users and IT companies, hence making protective state interventions all the more important. We thus urge to critically reflect on

privacy literacy discourses' tendency to support a shifting of responsibilities from the state to individuals. In fact, it should be vice versa due to the fact that only state agencies possess ample resources to initiate privacy protection and informational self-determination mechanisms that effectively harness IT companies, data brokers, foreign intelligence agencies, etc. It is obviously a mistake to blame individuals' poor privacy literacy skills and limited knowledge resources when they encounter information turbulence (Litt & Hargittai 2014) or context collapses that are due to revelations about surveillance programs, institutionalized data sharing, breaching of IT security, and the like. Of course, the discourse on privacy literacy does not devalue or disregard the importance of IT security or data protection agencies and regulations. Nevertheless, it may subtly evoke the notion that individual users have to take the protection of their informational privacy into their own hands (Hagendorff, 2018; Matzner et al., 2015). The untaught users have to be empowered; they must learn privacy techniques in order to escape their literacy deficiencies. However, average technology users are simply not capable of protecting personal data in all relevant regards. Generally speaking, more and more sensors and interconnected computing hardware became a ubiquitous component in people's environment. Thus, in a modern information society, it is virtually impossible for individuals to not become part of imperceivable tracking operations, machine learning predictions, data broker businesses, or, in general, "cyberspace" (Cuff, 2003).

In sum, protecting one's informational privacy is always dependent on others. First, there is no point in being privacy literate on one's own. Others have to engage in predictive privacy measures as well as interdependent privacy protection, too (Biczók & Chia, 2013; see also Trepte's as well as Petro & Metzgers' chapter on social and group privacy theories in this handbook). Second, users are dependent on IT security standards, data protection agencies, as well as data protection laws that effectively govern data collection practices by companies and other institutions. Only state institutions can come up with a staff of authorized experts who are not over-challenged by and capable of understanding information technologies, software code, laws, business models, security vulnerabilities, commercial data collection practices, etc. Privacy literacy may protect against a particular set of privacy risks, but state agencies can theoretically ensure a much more broad scope of privacy protection. For sure, they have conflicting interests since data protection as well as collection or surveillance serve different ministries' objectives. And one can even stress that privacy literacy comprises a precautionary principle that takes these conflicting interests into account. However, in the end, privacy protection resources are unevenly distributed, and data protection rights can protect especially those placed on the disadvantaged side of the digital divide. A process of "responsibilization" (O'Malley, 2009; Matzner et al., 2015), where accountability is transferred from the state to individuals, has problematic normative implications. Privacy risks should effectively be addressed not just on an individual, but also on a political level with its manifold instruments like binding legal norms, monetary incentives, subsidies, obligations for opt-out options, or the right to be forgotten. Eventually, in addition to empowering and educating individual users, IT companies should in reasonable parts be disempowered by these instruments in order to not just combat symptoms but also reach the root of privacy threats.

Future Perspectives and Conclusion

In this chapter, we reviewed the literature on online and social media privacy literacy, respectively, discussed methodical challenges surrounding their measurement, and critically evaluated the role of social media privacy literacy in safeguarding users' privacy. In this last section, we highlight some of our conclusions and provide avenues for future research.

Conceptually, we believe that research on online privacy literacy has come a long way. The field has matured from simple models focusing on fragmented dimensions of the broader concept to more comprehensive models that include specific knowledge dimensions, abilities, and skill sets. We see

the variety in conceptualizations as a testament to the vibrant research community that studies online and particularly social media privacy. In fact, we believe that different research questions and applications call for different concepts, levels of abstraction, and, conversely, levels of specificity with regard to its context. Nonetheless, we also believe that the question of how privacy literacy should be embedded within broader concepts such as computer and media literacy remains important. As we have seen, interventions for fostering privacy literacy are often embedded in broader educational resources on media literacy in general. The conceptual hierarchy and discriminant validity between media literacy and privacy literacy should hence be further investigated and discussed.

Methodologically, we have to conclude that there are only a few validated scales that measure online privacy literacy and hardly any scales that assess social media privacy literacy specifically (beyond short ad-hoc scales). OPLIS (Masur et al., 2017) remains one of the few objective measurement tools that nonetheless falls short in capturing the entirety of the discussed dimensions of online privacy literacy. A rigorously validated scale for *social* media privacy literacy is missing completely. This is problematic for various reasons: First, assessments of literacy levels in different populations may still be preliminary as ad-hoc scales and self-reports may contain measurement error and bias. Second, the true potential of social media privacy literacy in empowering individuals may still be underexplored. The preliminary evidence is again often based on subjective, rather than objective knowledge scales, and the more performative dimensions such as reflection ability or critical privacy literacy are not yet studied at all. We thus urge future research to engage in rigorous scale development and validation.

Empirically, the link between higher levels of social media privacy literacy and privacy behaviors on social media seems supported, but we lack causal and experimental investigations. The majority of work is based on cross-sectional survey designs. Beyond studying relationships between online privacy literacy and privacy behaviors, there is a lack of research on the role of privacy literacy in shaping prominently investigated privacy theories and processes. As mentioned before, the privacy paradox is commonly explained by a lack of skills and knowledge, but the empirical evidence is largely missing. We believe there are many opportunities for incorporating online privacy literacy as a key concept in many existing privacy frameworks. Among others, it may explain privacy decision-making as outlined in the privacy calculus (see, e.g., Dienlin & Metzger, 2016). It should likewise not be ignored when investigating heuristics and biases (see Liu et al., this volume) or how literacy and heuristic thinking may interact on a situational level (see chapter 6 by Masur in this volume).

Normatively, however, we caution against one-sided advocacy for online privacy literacy generally and social media privacy literacy specifically. Privacy literacy is often associated with individualistic notions about privacy and data protection. This is why it is only one albeit important measure that serves as a countermeasure against digital risks that are connected to issues of information control or the loss thereof. First and foremost, social media privacy literacy is concerned with frontend features of digital platforms, where users can engage with privacy settings, delete posts, un-tag photos, search for their content, manage profile visibility, etc. However, this must not lead to a disregard of privacy risks that are situated at the platforms' backends, meaning the "invisible" part of user communication, information exchange, machine learning, or data mining. Privacy settings that users can access are just the surface of what is relevant when managing digital privacy boundaries. This has to extend to the backends of platforms and services, to the algorithms, machine learning models, server centers, data brokers, intelligence agencies, etc., where social sorting (Lyon, 2003), algorithmic discrimination (Barocas & Selbst, 2016), AI-driven decision-making (Crawford et al., 2019), or micro-targeting (Matz et al., 2019) takes place. Future research should hence be clear about the (limited) potential of social media privacy literacy and outline what a higher literacy can and what it cannot achieve. Being transparent about both general online privacy literacy's and social media privacy literacy's strengths and weaknesses and its inherent limitations will help to better define its role in protecting user privacy while upholding the need to also engage in other, less individual-centered solutions.

Notes

1 see: www.oplis.de
2 see: https://osf.io/md8ch?view_only=b03665d09fd84f1393570e46dcf25f54
3 https://www.facebook.com/fbgetdigital
4 https://beinternetawesome.withgoogle.com/en_us/families
5 https://www.commonsense.org/education
6 e.g., https://www.lfk.de/medienkompetenz/social-media
7 https://www.bmfsfj.de/bmfsfj/themen/kinder-und-jugend/medienkompetenz
8 https://netwerkmediawijsheid.nl/kennis-tools/
9 https://www.socialmediatestdrive.org

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy enhancing technologies* (Vol. 4258, pp. 36–58). Lecture notes in computer science. Berlin: Springer. https://doi.org/10.1007/11957454_3

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

Baacke, D. (1996). Medienkompetenz: Begrifflichkeit und sozialer wandel. In A. von Rein (Hrsg.) (Ed.), *Theorie und praxis der erwachsenenbildung: Medienkompetenz als schlüsselbegriff* (pp. S112–S124). Bad Heilbrunn: Klinkhardt.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, *104*, 671–732.

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., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53.

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118–123. https://doi.org/10.1016/j.copsyc.2020.05.004

Biczók, G., & Chia, P. H. (2013). *Interdependent privacy: Let me share your data*. Berlin: Springer.

Binder, A., Stubenvoll, M., Hirsch, M., & Matthes, J. (2022). Why am I getting this ad? How the degree of targeting disclosures and political fit affect persuasion knowledge, party evaluation, and online privacy behaviors. *Journal of Advertising*, *51*(2), 206–222. https://doi.org/10.1080/00913367.2021.2015727

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences. *Social Psychological and Personality Science*, *4*(3), 340–347.

Crawford, K., Dobbe, R., Dryer, T., Fried, G., Green, B., Kaziunas, E., et al. (2019). AI now 2019 report. AI now. New York. Available online at https://ainowinstitute.org/AI_Now_2019_Report.pdf, checked on 12/18/2019.

Choi, S. (2022). Privacy literacy on social media: Its predictors and outcomes. *International Journal of Human–Computer Interaction*, https://doi.org/10.1080/10447318.2022.2041892

Chomsky, N. (1976). Conditions on rules of grammar. *Linguistic analysis*, *2*(4), 303–351.

Cuff, D. (2003). Immanent domain. Pervasive computing and the public realm. *Journal of Architectural Education*, *57*(1), 43–49.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzingself-disclosure and self-withdrawal in a U.S. representative sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. 10.1111/jcc4.12163

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society*, *6*(2). https://doi.org/10.1177/2056305120916853

Gambino, A., Kim, J., Sundar, S. S., Shyam, S., Ge, J., & Rosson, M. B. (2016). User disbelief in privacy paradox: Heuristics that determine disclosure. In J. Kaye, A. Druin, C. Lampe, D. Morris, & J. P. Hourcade (Eds.), *Proceedings of the 2016 CHI conference extended abstracts on human factors in computing systems – CHI EA: Vol. 16, 2892413* (pp. 2837–2843). New York, NY: ACM Press. https://doi.org/10.1145/2851581.

Groeben, N. (2002). Dimensionen der medienkompetenz: Deskriptive und normative aspekte. In N. Groeben & B. Hurrelmann (Hrsg.) (Eds.), *Medienkompetenz: Voraussetzungen, dimensionen, funktionen* (pp. S. 160–197). Weinheim: Juventa.

Gruzd, A., McNeish, J., Halevi, L. D., & Phillips, M. (2021). Seeing self in data: The effect of a privacy literacy intervention on Facebook users' behaviour. Available at SSRN: https://doi.org/10.2139/ssrn.3946376

Hagendorff, T. (2018). Privacy literacy and its problems. *Journal of Information Ethics*, *27*(2), 127.

Harborth, D., & Pape, S. (2020). How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *51*, 51–69. https://doi.org/10.1145/3380799.3380805

Higdon, N. (2021). The critical effect: Exploring the influence of critical media literacy pedagogy on college students' social media behaviors and attitudes. *Journal of Media Literacy Education Pre-Prints*. Retrieved from https://digitalcommons.uri.edu/jmle-preprints/3

Hobbs, R. (2010). *Digital and media literacy: A plan of action*. The Aspen Institute.

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies*. Retrieved from http://ssrn.com/abstract=1589864

Jeong, S.-H., Cho, H., & Hwang, J. (2012). Media literacy interventions: A meta-analytic review. *Journal of Communication*, *62*(3), 454–472. https://doi.org/10.1111/j.1460-2466.2012.01643.x

Kellner, D., & Share, J. (2005). Toward critical media literacy: Core concepts, debates, organizations, and policy. *Discourse: Studies in the Cultural Politics of Education*, *26*, 369–386. https://doi.org/10.1080/01596300500200169

Lambiotte, R., & Kosinski, M. (2014). Tracking the digital footprints of personality. *Proc. IEEE*, 102(12), 1934–1939.

Litt, E., & Hargittai, E. (2014). A bumpy ride on the information superhighway. Exploring turbulence online. *Computers in Human Behavior*, *36*, 520–529.

Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications*, *39*(3). https://doi.org/10.1515/commun-2014-0113

Lyon, D. (2003). Surveillance as social sorting. Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as social sorting. Privacy, risk, and digital discrimination* (pp. 13–30). London: Routledge.

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-78884-5

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und validierung der online-privatheitskompetenzskala (OPLIS) [engl. Development and validation of the online privacy literacy scale]. *Diagnostica*, *63*, 256–268. https://doi.org/10.1026/0012-1924/a000179

Matz, S. C., Appel, R. E., & Kosinski, M. (2019). Privacy in the age of psychological targeting. *Current Opinion in Psychology*, *31*, 116–121.

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Self-data-protection – empowerment or burden? In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Data protection on the move* (pp. 277–305). Springer: Netherlands. https://doi.org/10.1007/978-94-017-7376-8_11

Mühlhoff, R. (2021). Predictive privacy: Towards an applied ethics of data analytics. *SSRN Journal*, 1–24.

Nissenbaum, H. (2010). Privacy in context. In *Technology, policy, and the integrity of social life*. Stanford University Press.

O'Malley, P. (2009). Responsibilization. In A. Wakefield & J. Fleming (Eds.), *The SAGE dictionary of policing* (pp. 277–279). London: SAGE Publications Ltd.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology*, *17*, 147–156. https://doi.org/10.1006/jevp.1997.0049

Potter, W. J. (2010). The state of media literacy. *Journal of Broadcasting & Electronic Media*, *54*(4), 675–696. https://doi.org/10.1080/08838151.2011.521462

Purington Drake, A., Masur, P. K., Bazarova, N., Zou, E. W., & Whitlock, J. (2022). The youth social media literacy inventory: Development and validation using item response theory. *SocArXiv*. https://doi.org/10.31235/osf.io/wfnd7

Schäwel, J., Frener, R., & Trepte, S. (2021). Political microtargeting and online privacy: A theoretical approach to understanding users' privacy behaviors. *Media and Communication*, *9*(4), 158–169. https://doi.org/10.17645/mac.v9i4.4085

Schäwel, J., Frener, R., Masur, P. K., & Trepte, S. (2021). Learning by doing oder doing by learning? Die Wechselwirkung zwischen Online-Privatheitskompetenz und Datenschutzverhalten. *Medien & Kommunikationswissenschaft*, *69*(2), 221–246.

Schubert, R., Marinica, I., Mosetti, L., & Bajka, S. (2022). Mitigating the privacy paradox through higher privacy literacy? *Insights from a lab experiment based on Facebook data*. Retrieved from https://collegium.ethz.ch/wp-content/uploads/2022/05/Schubert-Marinica-Mosetti-Bajka-Mitigating-the-Privacy-Paradox2.pdf

Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online privacy literacy and online privacy behavior–the role of crystallized intelligence and personality. *International Journal of Human–Computer Interaction*, *37*(15), 1455–1466.

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication*, *22*(2), 26. https://doi.org/10.1111/jcc4.12182

Sutter, T., & Charlton, M. (2002). Medienkompetenz: Einige Anmerkungen zum Kompetenzbegriff. In N. Groeben & B. Hurrelmann (Hrsg.) (Eds.), *Medienkompetenz: Voraussetzungen, Dimensionen, Funktionen* (pp. S. 129–147). Weinheim: Juventa.

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*. https://doi.org/10.1016/j.chb.2019.08.022

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). Netherlands: Springer. https://doi.org/10.1007/978-94-017-9385-8

Turow, J. (2003). Americans and online privacy: The system is broken. A report from the Annenberg public policy center of the University of Pennsylvania. *Abgerufen unter*, https://repository.upenn.edu/cgi/viewcontent.cgi?referer=https://www.google.de/&httpsredir=1&article=1411&context=asc_papers

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470.

Weinert, F. E. (2003). *Leistungsmessungen in Schulen*. Weinheim, Basel: Beltz.