Definitions of privacy

Trepte, Sabine; Masur, Philipp K.

published in
The Routledge Handbook of Privacy and Social Media
2023

DOI (link to publisher)
10.4324/9781003244677-2

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

1
DEFINITIONS OF PRIVACY

Sabine Trepte[1] *and Philipp K. Masur*[2]

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

Introduction

Very often, scholarly work starts with the claim that the field has not yet settled on a uniform definition. We believe that struggling to define a core concept is not necessarily a problem, but rather a symptom of a lively and active field. Uniform definitions, in contrast, reflect that the concept is not important, draws little attention, or worse, is owned by a handful of scholars reigning over this field and normalizing its research. Fortunately, none of this is the case in research on privacy, online privacy, or social media privacy. Over the last 60 years, privacy has become a vibrant area of research, with a significant peak in research activities regarding privacy on social media after 2010. Since this time, many flagship articles, books, and chapters have been published (Eichenhofer, 2019; Masur, 2018; Nissenbaum, 2010; Papacharissi, 2010; Sevignani, 2016; Trepte & Reinecke, 2011). Consequently, we can conclude that privacy research is growing and very much alive, as evidenced by the existence of many different definitions of privacy.

With this chapter, we provide an overview of the most popular definitions of privacy and discuss these with regard to i) their theoretical background, ii) model of humanity, iii) their suitability for capturing social media privacy, and iv) how well they facilitate communication regarding aspects and issues related to social media privacy in applied contexts (i.e., to the press, the public). In line with our arguments above and the inherent nature of the term privacy, this chapter does not seek to establish a single, final definition, but rather discusses definitions that meet different criteria and as such add to the body of knowledge in the field of privacy and social media.

Seminal Definitions of Privacy

For several decades and even centuries, scholars have grappled with the task of defining privacy. To the non-academic reader, this may come as a surprise. After all, the meaning of something described as "private" is readily understood by everyone: We call something private that belongs to us and that is kept separate from others, such as our homes, our thoughts and feelings, or our intimate family life. Here, we use the descriptive meaning of the word. However, we also seek to emphasize that the private thing *should* not be accessed or known by others, certainly not by the general public. If we consider something private, it belongs to us and we get to decide what happens with it. Here, the word privacy is used in its normative meaning.

Nevertheless, pinpointing an exact scholarly definition of privacy is almost impossible, at best difficult. From an academic point of view, the variety of definitions reflects the different disciplinary

DOI: 10.4324/9781003244677-2

backgrounds and purposes for which concepts of privacy have been created. It is thus understandable that privacy is often conceived as a *right* when legal issues are at stake, as a *form of control* if behavioral processes are under investigation, and as *a state of seclusion* when psychological perceptions of privacy are studied.

That being said, there are nonetheless commonalities between the different approaches that are worthwhile to highlight before we review some of the seminal definitions of privacy. For example, almost all modern, Western concepts of privacy are rooted in the work of liberal theorists such as Hobbes (1651/2011), Locke (1689/2005), and Mill (1859/2015). In describing the boundaries of a state's or sovereign's power, they coined the idea of negative freedom: The sole purpose of intervening with people's liberty of action is protection (e.g., Mill, 1859/2015). Negative freedom is thus freedom from external (i.e., the state's) intervention. This idea often translates to concepts of privacy that emphasize protection from external influences (Masur, 2020; Rössler, 2001).

Legal scholars Warren and Brandeis (1890) paved the way to defining the actual term privacy when they demanded "the right to be let alone" (p. 195), meaning that privacy translates to freedom from intrusion by the press. Their essay inspired an international conversation on how to define privacy in law and beyond. Interestingly, their motivation was a changing media environment. Warren and Brandeis claimed that personal attitudes, sentiments, and interactions would be protected by the law, but that recording and publishing would not. Nevertheless, their definition is somewhat imprecise with regard to what privacy actually is. Is "being let alone" the right itself? Or is it "being let alone" that the right aims to protect? We will see that protection of being let alone and managing access to oneself constitute the basis for most of the seminal work on privacy. One of the most commonly cited definitions of privacy building on Warren and Brandeis stems from Westin who proposed the following definition from a legal point of view:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others […]. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.
>
> *(Westin, 1967, p. 5)*

We thus again observe ambiguity as Westin defines privacy as a broad legal claim, but also as a rather descriptive, reduced state of withdrawal. Furthermore, four states of privacy are introduced: Solitude, intimacy, anonymity, and reserve (Westin, 2003). Withdrawal as a function of privacy has become the basis for many psychologically inspired theories of privacy (Altman, 1975; Dienlin, 2014; Masur, 2018; Petronio, 2002).

The ambiguity in Westin's definition is also reflected in the growing amount of privacy literature in the 1960s–1990s. Over the years, a fruitful debate between what could be termed an anti-reductionist perspective (e.g., DeCew, 1997; Prosser, 1960; Solove, 2008) vs. a reductionist perspective (Allen, 1988; Gavison, 1980; Miller, 1971) emerged. The former argued that privacy touches upon too many aspects and areas and can therefore not be boiled down to a single definition. In other words, anti-reductionists highlight the necessity of taking the circumstances of a specific situation and contextual factors into account when trying to identify privacy values and interests. Solove (2008), for example, proposed a pluralistic understanding of privacy, stating that we should no longer search for one unifying common trait in all privacy violations, as one "can identify many specific elements of privacy without sacrificing inclusiveness" (Solove, 2008, p. 44).

Reductionists, in contrast, often held extreme positions such as abandoning the term privacy altogether for its lack of precision and overall vagueness. Their reduced definitions describe privacy

as a state or condition. Gavison (1980), for example, defined privacy as "the limitation of others' access to an individual" (p. 428). Reductionists often argued that such a reduced, primarily descriptive concept of privacy can help to establish objective criteria for different levels of privacy.

Within the social sciences, work by Altman (1975) has been most influential in shaping definitions of privacy:

> For my purpose, privacy will be defined as the selective control of access to the self or to one's group.
>
> *(Altman, 1975, p. 18)*

Again, we observe a vagueness as to what privacy actually is. Is privacy really an individual's active control of access, or is it again a condition of limited access to this person, or both? Altman (1975) of course disentangles these questions in his work. And Irvin Altman inspired the analysis of privacy as a constant process of interpersonal boundary control aimed at optimizing levels of access to the self in alignment with one's personal needs for seclusion and interaction. The metaphor that "Privacy regulation by persons and groups is somewhat like the shifting permeability of a cell membrane" (Altman, 1975, p. 10) continues to be a useful metaphor for the shifting needs and circumstances that people deal with today (e.g., as laid out in Communication Privacy Management Theory, by Petronio, 2002; see further as follows).

With the rise of computers and later the internet, privacy scholars began to emphasize what Warren and Brandeis had earlier discovered as a conceptual gap in lawmaking, that is, the flow of information and "informational privacy." For example, Miller (1971) noted

> […] that the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him—a power that often is essential to maintaining social relationships and personal freedom.
>
> *(Miller, 1971, p. 25)*

Privacy definitions from this time reflect growing concerns over governments' and institutions' ability to collect and store personal information.

Consolidating different perspectives on privacy and relying on the work of the scholars denoted above, Burgoon (1982) proposed a multi-dimensional concept of privacy that differentiates between individuals' control over information, physical distance, social interaction, and the psychological experience of privacy. Here, *informational privacy* is defined as an individuals' ability to control the initial release of information about themselves and its subsequent distribution and use. Burgoon highlights that the amount of information in others' hands, its content, and the nature and relationships with those possessing the information are relevant. This also relates to the dimension of *social privacy*, an individual's ability to control the pattern of social contacts on an individual, dyadic, or group level. Social privacy varies with the "degree of personalness of conversational topics and language" (p. 222). *Psychological privacy* is defined as an individual's "ability to control affective and cognitive input and outputs" (p. 224). Finally, *physical privacy* refers to an individual's ability to control and choose the limits of one's physical boundaries to others, the "freedom from intrusion to one's self-defined body-buffer zone" (p. 211).

According to Margulis (2011), one of the most valuable theories for studying privacy in online environments is Communication Privacy Management Theory (Petronio, 2002):

> In this theory, privacy is defined as the feeling that one has the right to own private information, either personally or collectively; consequently, boundaries mark ownership lines for individuals.
>
> *(Petronio, 2002, p. 6)*

This idea of ownership is central to the theory. Privacy management thereby entails sustaining and controlling private boundaries with other people. The limits of such boundaries are defined by specific rules that coordinate the level of accessibility of the information that flows between group members defining the boundary.

As the above literature review has shown, general definitions of privacy are manifold. Over time, they have been refined, adapted, and adjusted. In light of this, the best course of action may well be to adopt an anti-reductionist approach and consider all of these definitions as worthwhile starting points and fruitful in their own right. As Margulis noted: "If you intend to use a behavioral theory of privacy, you should determine whether its definition of privacy meets your requirements" (Margulis, 2011, p. 15). We believe that the plurality of definitions is not necessarily a weakness, but rather a strength of our field. The richness of the ideas in the work referred to above and the many more we could not cite due to the word limitations of this chapter have undoubtedly shaped the work of the authors in this volume. As has been done in the past, we believe that we should continue to place our definitions of privacy under scrutiny and examine their potential to explain and describe current practices, phenomena, and processes. In what follows, we highlight how scholars have used these seminal definitions of privacy and adapted them to reflect the specificities of online environments and specifically the reality of managing privacy on social media.

Defining Online Privacy

We have demonstrated how seminal privacy research has laid the groundwork for our current understanding of privacy and can be understood as the first pillar of current privacy research. We would consider early research in computer-mediated communication the second pillar of our current understanding of privacy (Joinson, 2001; Joinson et al., 2006; Tidwell & Walther, 2002). Ironically, this early work seldom explicitly mentioned the term privacy. It was strongly centered around the individual agent, processes of how an individual reacts to certain circumstances with disclosure or withdrawal, and of course, the context was not yet social media, but rather online forums (Barak & Gluck-Ofri, 2007). Here, computer-mediated interpersonal communication could be observed and investigated in a nutshell.

Privacy was pivotal to communication science in the first decade of the millennium because it was at risk. The commercial internet had started to develop and jurisprudence was always one step behind what developers had invented (Sevignani, 2016). Data was considered the new oil (The Economist, 2017). Hence, the most important scholarly work on online privacy in these early years was published with respect to individual regulation on the one hand and e-commerce on the other (Acquisti, 2005; Acquisti & Grossklags, 2004; Ben-Ze'ev, 2003; Dinev & Hart, 2004, 2006; Dommeyer & Gross, 2003; Jensen et al., 2005; Metzger, 2004; Palen & Dourish, 2003; Patil & Kobsa, 2005; Preibusch, 2006; Tavani & Moor, 2001; Viegas, 2005). Here, scholars strove to understand the ways in which privacy was perceived, enacted, controlled, or violated in "cyber-space," the "networked world," or simply "the internet." Thus, the internet was conceptualized in a rather abstract way.

What do these developments tell us with regard to definitions of privacy? In retrospect, it seems that the full force of research was directed towards understanding privacy in online realms in the very broadest sense, with no further adaptations of privacy definitions for this new context. Definitions were mostly drawn from the seminal theories we referred to in the previous section and applied to how individuals regulate privacy with regard to service providers.

Only later, when social media became as dominant as the mass media, did scholars realize that privacy experienced in online media cannot always be fully captured by the definitions already in use. Only then did they suggest privacy definitions specifically tailored to the online applications, services and experiences(Acquisti & Gross, 2006; Barnes, 2006; Gross & Acquisti, 2005; Nissenbaum, 2010;

Papacharissi, 2010, 2011; Reinecke et al., 2008; Sevignani, 2016). Interestingly, these online privacy definitions were tremendously influencedby social media practices and scholarship. Hence, the term online privacy did not have a definition in its own right that we would consider a well-established or important step of privacy theorizing.

Defining Privacy for the Social Media Context

Central to this handbook is the question of how privacy can be defined for the context of social media. In what follows, we therefore first seek to establish the context and discuss the existing definition of social media in general and social networking sites in particular. We then discuss how the specific characteristics, affordances, and boundary conditions of social media need to be considered when defining privacy for social media. We thereby particularly emphasize that social media and privacy are inherently social, dynamic, and at their core rooted in communication between individuals as well as with companies and institutions. We will discuss the nature and flow of social media use based on the central tenets of the Social Media Privacy Model (Trepte, 2021) and illustrate each step with associated research. This will allow us to review definitions of privacy for the social media context that we believe incorporate the particularities of privacy in social media and provide sufficient complexity for future research.

Social Media

To start with, it is important to better understand the context in which privacy became relevant after 2005, when the social media emerged as a global, popular, and ubiquitous phenomenon. What defines the technology and as such the context in which users now find themselves spending many hours of the day? A very commonly cited definition underlines users' activities and social media affordances:

> Social media are Internet-based channels that allow users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others.
>
> *(Carr & Hayes, 2015, p. 50)*

In their definition, Caleb T. Carr and Rebecca A. Hayes underline that social media have four discrete requirements. They 1) consist of online platforms that 2) support synchronous and asynchronous communication, 3) are social in nature, and 4) are primarily based on user-generated content. We endorse the definition because it views technology as a context affording interaction. This definition encompasses what we think is key to understanding social media privacy as well: Technology is co-developed through interactions among users themselves, but also by developers reacting to these users' interactions. In social media, there is no clear "regime" of technology (see chapter 6 by Masur on situational privacy and chapter 9 by Treem, van Zoonen, and Sivunen on social media affordances and privacy). Rather, technology is both socially shaped and socially shaping (Williams, 1974), and its uses are negotiated among individuals, society, and the technology itself (Papacharissi, 2012). Similarly, how privacy is perceived and negotiated is shaped by technology *and* through social media users' practices.

Whereas social media can be seen as an umbrella term including various platforms and services, the perhaps most prominent examples are social networking sites such as Instagram, Twitter, Mastodon, BeReal, Snapchat, and Facebook.

> A social networking site is defined as a "[…] networked communication platform in which participants 1) have uniquely identifiable profiles that consist of user-supplied content, content provided by other users, and/or system-level data; 2) can publicly articulate connections that can be viewed and traversed by others; and 3) can consume, produce, and/or interact with streams of user-generated content provided by their connections on the site".
>
> *(Ellison & boyd, 2013, p. 158)*

In this definition of social networking sites, the interactional and social aspects of use practices are emphasized, highlighting users' profiles, connections, and behaviors. Here, social media are understood as an inherently social matter. Interestingly, although Carr and Hayes' social media definition as well as Ellison and boyds' definition of social networking sites seek to conceptualize a technology, most words actually refer to people and their practices in using it. From our point of view, this is no coincidence and is an important feature of definitions aiming to capture the fluctuating and dynamic nature of both social media and (as described in the following section) privacy, respectively.

Defining Privacy in Social Media

In the next step, we can investigate which interactions among individuals, dyads, groups, and collectives are relevant for the experience and practice of privacy on social media. From 2010 on, individuals negotiating and managing their personal privacy needs in light of the internal and external demands of social media use have been at the core of privacy research. In the "Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web" (Trepte & Reinecke, 2011) – the book preceding this handbook – each of the 18 chapters refers to the negotiation of social media privacy. Authors describe social media users' struggles to attain or regain privacy on the one hand and to engage in self-presentation, emancipation, and inclusion on the other. In the introduction to the book, Margulis (2011) critically notes that the three most popular seminal definitions of privacy by Westin, Altman, and Petronio are of limited generalizability, because they cannot sufficiently be applied to the social media context.

A pivotal perspective on how privacy could be understood and defined in a networked, modern democracy was proposed by Zizi Papacharissi (2010) in "A private sphere: Democracy in a digital age," in which the convergence of economic, cultural, social, and political contexts is discussed along the lines of three themes: First, that "the privacy realm as a personal domain [is] presently contested by profit-driven objectives, thus leading to a potential commodification of *privacy*" (p. 42ff); second, that we are witnessing a "privatization of the public space" (p. 37ff) and "a progression towards a more intimate society" (p. 42); third, that "the rejection of both public and private spaces for the pursuit of a malleable space in between, characterized by activity that is *social* at heart, but that could embed political/civic merit and consequences" (p. 37). Social media use can well be seen as a key driver of the phenomena described in these themes. Although not specifically providing a definition of social media privacy, this analysis clearly paved the way for more specific and contextualized conceptualizations.

Nissenbaum (2010), who discussed privacy in the context of modern information and communication technologies, likewise provides a new perspective on privacy that takes the fluctuating and social nature of social media into account. In an attempt to emphasize the contextuality of privacy, Nissenbaum (2010) advanced the theory of contextual integrity, in which privacy is an individual's claim to an appropriate flow of information in a given context, arguing that there is great variability in a person's privacy needs that are systematically linked to the prevailing social context. A privacy violation is thus not necessarily a form of unwanted

access, as often suggested by earlier theories (see above), but rather inappropriate access given a respective context:

> We have a right to privacy, but it is neither a right to control personal information nor a right to have access to this information restricted. Instead, it is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met […].
>
> *(Nissenbaum, 2010, p. 231)*

In 2010, Nissenbaum reflected on privacy against the backdrop of new technologies, including social media. This definition claims privacy as a right, as claimed 120 years earlier by Warren and Brandeis. It also coincides with Altman's and Westin's idea that individuals should strive to meet their ideal level of personal information flows. Yet, it further specifies contextual factors, including role perceptions, norms, and values that determine the principles of information flow in a given context.

The importance of acknowledging the specific context and affordances of social media use was underlined by danah boyd, who argued that

> […] achieving privacy requires the ability to control the social situation by navigating complex contextual cues, technical affordances, and social dynamics. Achieving privacy is an ongoing process because social situations are never static.
>
> *(boyd, 2014, p. 60)*

Of course, situations are never static. Situational experiences also differ in non-mediated environments. However, early research on social media and privacy often assumed that these platforms are somewhat static, with everything remaining just as it was designed by the platform developers, unless the same or another developer steps in to make a change. This perspective often failed to acknowledge that within social media, people experience vastly different situations although using the exact same technology. Some communicative acts have small, others large or even unknown audiences. Some conversations are not accessible to others (e.g., in signal via end-to-end encryption), while others are protected by the cloak of anonymity (e.g., posting something under a pseudonym). Thus, no social media use episode (even within a single platform) is the same, which requires users to constantly evaluate their level of privacy and the options they have available to control it. This idea of fluctuating context is highlighted in Masur's (2018) situational definition of privacy:

> Privacy is a subjective perception resulting from the characteristics of the environment in which an individual happens to be at a given time. More precisely, the entirety of interpersonal and external circumstances (and their interactions) determines what level of privacy an individual perceives.
>
> *(Masur 2018, p. 312)*

Privacy practices thus are deeply embedded in the technical and social architecture of social media platforms. These specific contexts and the situations they typically produce have to be considered when aiming to understand how social media users perceive, enact, and regulate their privacy. But what exactly does this intricate interplay between social media use and privacy look like?

We outline the major tenets of the Social Media Privacy Model (Trepte, 2021) and adjacent research to highlight more explicitly how privacy is perceived and enacted on social media (Dombrowski & Trepte, 2023; Schäwel et al., 2021; Trepte & Dombrowki, 2023).

The privacy-relevant process of social media use starts with an initial assessment: Individual users assess their *ideal level of access* to the self, as laid out by the theorists referred to above (Altman, 1975; Gavison, 1980; Petronio, 2002). The ideal level of access refers to people's preference for how much should be known about themselves at a given moment in time. It is quantifiable in the sense of more or less (or alternatively, high or low). It results from individuals' dispositions (e.g., their individual need for privacy, personality, and experiences) and more external requirements and situational demands.

Then, social media users have different privacy-relevant *communication goals*, such as information retrieval, exchange of content, or simply socializing with other users. These goals come along with different challenges for privacy regulation and vary with regard to the gratifications to be expected from others (Trepte et al., 2020). Furthermore, time pressure is often an issue in privacy regulation and can crucially alter communication goals (see chapter 8 on heuristics in privacy decision-making by Liao, Sundar, and Rosson). In sum, one's initial assessment of the ideal level of access and one's communication goals set the expectations and motives, they are the glasses that social media users wear when evaluating social media interactions.

Social media boundary conditions exist in terms of content, the flow of content, and uses. First, what content social media users find online is the most important and first issue they deal with. Then comes the *flow of content* and how it is, will, or might be monitored and used, both by other social media users and also by third parties such as companies, service providers, or even state authorities. The exchange of information with other users on social networking sites is stored on servers owned by the platform providers and saved on other users' profiles; it can be forwarded, published to a wider audience, deleted, or move outside the internet.

Affordances set the boundaries of what is possible with regard to privacy regulation and what social media users can do to safeguard and regulate their privacy in alignment with their individual level of access and communication goals (Trepte, 2015). Affordances can be defined as the result of the interaction between the possibilities and features of the social media context on the one hand, and how social media users breathe life into these features on the other (Fox & McEwan, 2017; Treem & Leonardi, 2012). The affordance of anonymity, for example, means that social media users participate, get in touch with one another, interact, and retrieve information with varying degrees of identifiability, but this comes at the price of not being identifiable and thus not oneself. Editability means that in the course of using social media, individual actions are changeable and can be edited and altered. Association, as the core social media affordance, means that the content of social media and its flow allows for and demand interaction with others. Only those deliberately sharing their identity and more will be rewarded with what has been shown to make social media users happy and healthy: Social contacts (Dienlin et al., 2017). Persistence means that content is more or less available over time. All of these affordances are deeply social. They are rooted in social processes and are expressed as such. Consequently, not only how the structures of social media are designed for social encounters, but also how they are used in practice, are driven by social processes. Social encounters determine how social media features work.

Affordances such as anonymity, editability, association, and persistence define *privacy mechanisms*, or in other words, the options individuals have at their hands to regulate their privacy and to rely on: Control, trust, norms, and interpersonal communication. With the emergence of social media, it became clear to both scholars and users that control is only one of the privacy mechanisms (Hargittai & Marwick, 2016; Tavani & Moor, 2001). Accordingly, control, but also trust and norms, can be considered the most important privacy mechanisms that social media users tend to rely on. Then, the option to communicate about one's privacy has been discussed as an important mechanism in more current privacy theorizing and empirical studies (de Wolf, 2020; Trepte, 2021).

Users want to share personal information with others in order to celebrate life or share sadness and sorrow. To do so, they have to rely on social and legislative norms asserting that these pieces of

information will not find their way into information flows that betray them and these purposes. When assessing the boundary conditions, they think about whether they can trust other users, how much they can rely on established norms, or whether it would be better to get in touch with other users in order to personally explain that this specific picture or piece of information should not be shared with (certain) others. Privacy mechanisms are nothing more than options in this step. Each individual's assessment of their communication goals and of the social media boundaries results in an assessment of what can be done, what is necessary, and what is available with regard to privacy regulation. Then, in the next step, the situational and experienced level of access is re-assessed, leading to the individual perception of privacy in this certain situation, as outlined in Masur's (2018) definition of privacy. Only if an individual is aware of their individual goals and the social media boundaries can they determine how they feel about their individual privacy and whether and how they should regulate their privacy in the following.

Privacy regulation behaviors have often been used synonymously with privacy in respective definitions. According to the Social Media Privacy Model, such behaviors include "interdependent" and more "ego-centered" forms of regulation (Trepte, 2021). First, interdependent privacy regulation behaviors include deliberation, institutionalized, and often public communication. Here individual privacy regulation can become a part of the democratic process. Deliberation is widely known and theorized in the field of political communication, and scholars always found that privacy is political (Ochs, 2018; Papacharissi, 2010). Privacy refers to the freedom of social media users and of larger networks and as such has important political dimensions. Second, the most important form of privacy regulation on social media is *interpersonal communication*. Examples of this include a brief check-in among colleagues about how to handle sharing private pictures after a work event or a longer talk about pictures of a young couple on one of their Instagram's (de Wolf, 2020).

Ego-centered forms of privacy regulation, including control and self-disclosure, are much more commonly discussed in theorizing and definitions. *Control* means that social media users take advantage of their option to consent, correct information, or adjust access and protection (Tavani, 2007). On social media, there is only a very narrow space for controlling who shares what with whom. Although not much control is available, social media users still feel that controlling information is one of the most efficient and certainly the easiest way of obtaining the experience of privacy they expect (Sarikakis & Winter, 2017).

Self-disclosure has been key to understanding privacy online and on social media ever since (Dienlin & Metzger, 2016; Joinson, 2001). Self-disclosure is thus the most researched form of privacy regulation because, without self-disclosure, social media participation is not visible and not executable. Each and every step of social media use involves self-disclosure, from registration to logoff. Hence, self-disclosure is often not a conscious or pro-active form of privacy regulation, but first and foremost active participation on social media implying granular forms of disclosure and withdrawal.

Although we believe these are the most important regulation behaviors, there are of course more. Withdrawal has been introduced as the counterpart to self-disclosure (Dienlin & Metzger, 2016; Meier et al., 2020). Also, legal measures are sometimes a necessary step of privacy regulation when other regulation behaviors fail. Furthermore, cognitive or emotional regulation accompanies other forms of regulation behavior and is sometimes only available approach (Dombrowski & Trepte, 2023). Cynicism and resignation do not encompass privacy behaviors, but can also be considered a type of privacy regulation because they involve a form of coping (see chapter 13 by Ranzini, Lutz, and Hoffmann). These privacy regulation behaviors – and this is a challenge for its empirical investigation – are not used in an on- or off-fashion, but rather intertwined.

Based on these considerations, Trepte (2021) developed a definition of social media privacy that specifically acknowledges the social, dynamic, and fluctuating nature of privacy during social media use:

> I define privacy by an individual's assessments of (a) the level of access to this person in an interaction or relationship with others (people, companies, institutions) and (b) the availability of the mechanisms of control, interpersonal communication, trust, and norms for shaping this level of access through (c) self-disclosure as (almost intuitive) behavioral privacy regulation and (d) control, interpersonal communication, and deliberation as means for ensuring (a somewhat more elaborated) regulation of privacy. In social media, then, the availability of the mechanisms that can be applied to ensure privacy are crucially influenced by the content that is being shared and the social media affordances that determine how this content is further used.
>
> *(Trepte, 2021, p. 561)*

In accordance with seminal and also most current theories, we consider the initial individual assessment of needs, access, and communication goals as the first step in defining the ideal level of privacy. We then argue that social media realms impose three relevant aspects for consideration – the other people involved, the content being shared, and the affordances encountered – and that social media users regulate their privacy in light of these aspects.

Conclusion

This chapter has pursued three goals. One was the rather service-oriented idea of reviewing definitions for other scholars, perhaps particularly those new to our field and seeking to gain first insights. Our second goal was to critically reflect on how these definitions serve different purposes. Lastly, we discuss the specific nature of privacy in the context of social media and finally suggest a definition that reflects social media privacy specifically. A definition is nothing more than a first attempt to find common ground and a starting point. Some are specific to certain aspects of privacy on social media, others are broad and all-encompassing. However, all definitions make it possible to conduct comparative research, which in turn advances the opportunity to conduct replication studies and compare findings. Most importantly, we believe it is important to embrace complexity in future privacy theorizing.

References

Acquisti, A. (2005). Privacy in electronic commerce and the economics of immediate gratification. In J. Breese, J. Feigenbaum, & M. Seltzer (Eds.), *EC ' 05: Proceedings of the 6th ACM conference on electronic commerce, June 5–8, 2005* (p. 21). Vancouver, Canada, ACM. https://doi.org/10.1145/988772.988777

Acquisti, A., & Gross, R. (2006). Awareness, information sharing, and privacy on the Facebook. In *56th Annual Meeting of the International Communication Association*, June 21–24, 2006, Dresden, Germany.

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior: Losses, gains, and hyberbolic discounting. In L. J. Camp & S. Lewis (Eds.), *Advances in information security: Vol. 12. Economics of information security* (pp. 165–178). Kluwer. https://doi.org/10.1007/1-4020-8090-5_13

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society. New feminist perspectives series*. Rowman & Littlefield.

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

Barak, A., & Gluck-Ofri, O. (2007). Degree and reciprocity of self-disclosure in online forums. *CyberPsychology & Behavior*, *10*(3), 407–417.

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

Ben-Ze'ev, A. (2003). Privacy, emotional closeness, and openness in cyberspace. *Computers in Human Behavior*, *19*(4), 451–567. https://doi.org/10.1016/S0747-5632(02)00078-X

boyd, d. (2014). *It's complicated. The social lives of networked teens*. Yale University Press.

Burgoon, J. K. (1982). Privacy and communication. *Communication Yearbook*, *6*(4), 206–249. https://doi.org/10.1080/23808985

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic Journal of Communication*, *23*(1), 46–65. https://doi.org/10.1080/15456870.2015.972282.

de Wolf, R. P. (2020). Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media & Society*, *22*(6), 1058–1075. https://doi.org/10.1177/1461444819876570

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press.

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Karl Stutz.

Dienlin, T., Masur, P. K., & Trepte, S. (2017). Reinforcement or displacement? The reciprocity of FtF, IM, and SNS communication and their effects on loneliness and life satisfaction. *Journal of Computer-Mediated Communication*. Advance online publication. https://doi.org/10.1111/jcc4.12183

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

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dombrowski, J., & Trepte, S. (2023). Predicting privacy regulation behavior on social media. *Under Review*.

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, *17*(2), 34–51. https://doi.org/10.1002/dir.10053

The Economist (2017). *The world's most valuable resource is no longer oil, but data*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Eichenhofer, J. (2019). *e-Privacy - Theorie und Dogmatik eines europäischen Privatheitsschutzes im Internet-Zeitalter [Theoretical and doctrinal foundations of a European privacy protection regulation in the internet age]*. University of Bielefeld.

Ellison, N. B., & boyd, d. (2013). Sociality through social network sites. In W. H. Dutton (Ed.), *The Oxford handbook of studies* (pp. 151–172). Oxford University Press.

Fox, J., & McEwan, B. (2017). Distinguishing technologies for social interaction: The perceived social affordances of communication channels scale. *Communication Monographs*, *84*(3), 298–318. https://doi.org/10.1080/03637751.2017.1332418

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

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In V. Atluri, S. Di Capitani Vimercati, & R. Dingledine (Chairs), *The 2005 ACM Workshop*, Alexandria, VA, USA.

Hargittai, E., & Marwick, A. E. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.

Hobbes, T. (1651/2011). *Leviathan*. Pacific Publishing Studio.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1–2), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, *31*(2), 177–192. https://doi.org/10.1002/ejsp.36

Joinson, A. N., Paine, C., Buchanan, T., & Reips, U.-D. (2006). Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *Journal of Information Science*, *32*, 334–343.

Locke, J. (1689/2005). *A letter concerning toleration*. Digireads.com Publishing.

Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 9–17). Springer.

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer International Publishing.

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

Meier, Y., Schäwel, J., Kyewski, E., & Krämer, N. C. (2020). Applying protection motivation theory to predict Facebook users' withdrawal and disclosure intentions. *SMSociety'20: International Conference on Social Media and Society*, 21–29. https://doi.org/10.1145/3400806.3400810

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4). https://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Mill, J. S. (1859/2015). *On liberty*. CreateSpace.

Miller, A. R. (1971). *The assault on privacy: Computers, data banks, and dossiers*. University of Michigan Press.

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

Ochs, C. (2018). Self-protection beyond the self: Collective privacy practices in (big) datascapes. In *Routledge research in information technology and society: Vol. 21. The politics and policies of big data: Big data, big brother?* (1st ed., pp. 265–291). Routledge.

Palen, L., & Dourish, P. (2003). Unpacking 'privacy' for a networked world. In V. Bellotti (Ed.), *CHI letters: Vol. 1, CHI 2003: Proceedings of the SIGCHI conference on human factors in computing systems* (5th ed., pp. 129–136). ACM Press. https://doi.org/10.1145/642611.642635

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age*. Polity Press.

Papacharissi, Z. (2011). *A networked self: Identity, community, and culture on social network sites*. Routledge.

Papacharissi, Z. (2012). A networked self: Identity performance and sociability on social network sites. In F. L. F. Lee , L. Leung ,J. L. Qiu ,& D. S. C. Chu (Eds.), *Frontiers in new media research* (pp. 207–221). Routledge Taylor & Francis.

Patil, S., & Kobsa, A. (2005). Uncovering privacy attitudes and practices in instant messaging. In M. Pendergast, K. Schmidt, G. Mark, & M. Ackerman (Eds.), *Proceedings of the 2005 international ACM SIGGROUP conference on supporting group work - GROUP '05* (p. 109). ACM Press. https://doi.org/10.1145/1099203.1099220

Petronio, S. (2002). *Boundaries of privacy*. State University of New York Press.

Preibusch, S. (2006). Implementing privacy negotiations in E-commerce. In X. Zhou (Ed.), *Lecture notes in computer science: Vol. 3841. Frontiers of WWW research and development: Proceedings* (Vol. 3841, pp. 604–615). Springer. https://doi.org/10.1007/11610113_53

Prosser, W. L. (1960). Privacy. *California Law Review*, *48*(3), 383–423. https://doi.org/10.2307/3478805.

Reinecke, L., Trepte, S., & Behr, K.-M. (2008). Web 2.0 users' values and concerns of privacy. In *58th Annual Conference of the International Communication Association (ICA), May 22–26, 2008*, Montreal, Canada.

Rössler, B. (2001). *Der Wert des Privaten* (1530th ed.). Suhrkamp.

Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media + Society*, *3*(1), 1–14. https://doi.org/10.1177/2056305117695325

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

Sevignani, S. (2016). *Privacy and capitalism in the age of social media. Routledge research in information technology and society: Vol. 18*. Routledge.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

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

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society*, *31*(1), 6–11. https://doi.org/10.1145/572277.572278

Tidwell, L. S., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations. Getting to know one another a bit at a time. *Human Communication Research*, *28*(3), 317–348. https://doi.org/10.1111/j.1468-2958.2002.tb00811.x

Treem, J. W., & Leonardi, P. M. (2012). Social media use in organizations. Exploring the affordances of visibility, editability, persistence, and association. *Communication Yearbook*, *36*, 143–189. https://doi.org/10.1080/23808985.2013.11679130

Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media and Society*, *1*(1), 1–2. https://doi.org/10.1177/2056305115578681

Trepte, S. (2021). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, *31*(4), 549–570. https://doi.org/10.1093/ct/qtz035

Trepte, S., & Dombrowki, J. (2023). Testing the social media privacy model. A meta-analysis. *In Preparation*.

Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy online. Perspectives on privacy and self-disclosure in the social web*. Springer.

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*, 106115. https://doi.org/10.1016/j.chb.2019.08.022

Viegas, F. B. (2005). Bloggers' expectations of privacy and accountability. An initial survey. *Journal of Computer-Mediated Communication*, *10*(3), article 12. https://doi.org/10.1111/j.1083-6101.2005.tb00260.x

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*. Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Williams, R. (1974). *Television: Technology and cultural form*. Fontana.