Article

Normative Paradoxes of Privacy: Literacy and Choice in Platform Societies

Paula Helm

Goethe-University Frankfurt, Germany
helm@em.uni-frankfurt.de

Sandra Seubert

Goethe-University Frankfurt, Germany
seubert@soz.uni-frankfurt.de

Abstract

Privacy scholars, advocates, and activists repeatedly emphasize the fact that current measures of privacy protection are insufficient to counter the systemic threats presented by datafication and platformization (van Dijck, de Waal, and Poell 2018: 24). These threats include discrimination against underprivileged groups, monopolization of power and knowledge, as well as manipulation. In this paper, we take that analysis one step further, suggesting that the consequences of inappropriate privacy protection online possibly even run counter to the normative principles that underpinned the standard clause for privacy protection in the first place. We discuss the ways in which attempts at protection run the risk of producing results that not only diverge from but, paradoxically, even distort the normative goals they intended to reach: informational self-determination, empowerment, and personal autonomy. Drawing on the framework of “normative paradoxes,” we argue that the ideals of a normatively increasingly one-sided, liberal individualism create complicities with the structural dynamics of platform capitalism, which in turn promote those material-discursive practices of digital usage that are ultimately extremely privacy-invasive.

Introduction

Privacy is generally defined as personal control over information and access.¹ In light of this function, privacy is further understood to be of instrumental value because it is necessary for personal autonomy and perceived as an integral component of individual self-determination. In line with these convictions, liberal democratic states have established a variety of legal frameworks and reformative endeavors like the new GDPR in the EU to protect and enhance privacy. However, most of these privacy regimes—both old and new—are insufficient to meet the challenges posed by new information technologies with their data mining and processing capabilities. This paper deals with the question of why privacy, despite a diversity of reformative protection measures, is still being diagnosed as in a crisis so fundamental that some commentators have even considered it to be dead.²

¹ Different variations of this very general framing can be found in Fried (2009), Solove (2008), Reiman (1995), and Westin (1967). One can also draw a rough distinction between an Anglo-American liberal understanding of privacy and a Continental-European one (Gusy, Eichenhofer, and Schulte 2016). Since the main companies currently dominating the internet, and thus the most contested sphere of privacy protection, are based in the United States, we are most concerned with their understanding of privacy protection. At the same time, though, we acknowledge that there are significant differences between the European and the US-American interpretations of privacy protection. For an account of this distinction, see, for instance, Whitman (2004). We also acknowledge that there are other cultural differences in the understanding of privacy that we cannot integrate within the scope of this paper (Busch 2015).

² Privacy has been declared dead—not just once, but multiple times. In 1999, for instance, McNealy (CEO of Sun Microsystems) stated, “you already have zero privacy—get over it” (qtd. in Sprenger 1999).

In posing this question, we base this paper on the general assumption that privacy and an appropriate form of privacy protection are essential, not only for individual freedom but also for the integrity of social life and thus the functioning of democratic and just societies. Nevertheless, our starting point is also a very skeptical one: fundamentally questioning prevailing understandings of privacy and the current ways in which privacy protection is being put into practice.

That said, we would like to go one step further than those who argue that current policies are not strong enough to provide adequate privacy protection. We argue that not only are current privacy protection regimes insufficient, but they also—and this is even more problematic—tend to have unintended, ambivalent, and often even paradoxical consequences for actors and societies. Nevertheless, we are also aware that discourses in this field do indeed demonstrate a sensitivity to the problems we are observing. We therefore suggest that many reformative measures in the field of privacy regulation can be seen as ongoing attempts to overcome the aforementioned problems. In this paper, we will analyze, discuss, and evaluate them as such.

We begin with a conceptual introduction to the notion of “privacy” and how it is being situated within today’s information societies (which we characterize as platform societies). We then look more specifically at two practical examples in which privacy protection is currently being put into practice: the “Notice and Choice” regime and programs that aim to expand and improve “digital literacy” in civil society. In our examination of these two examples, we proceed as follows: Firstly, we reconstruct the aims behind these privacy regulation measures and elaborate the type of normative principles that motivate these actions. Secondly, we analyze the extent to which these measures are capable of fulfilling their normative aims and show how they, deviating from their original or explicit intention, run the risk of producing unintended outcomes.

In our analysis of these two case studies, we draw on the concept of “normative paradoxes” developed by Axel Honneth and Ferdinand Sutterlüty (2015). This more broadly aligned concept helps us to contextualize some of the problematic and even ambivalent outcomes that we observe when analyzing recent privacy protection regimes. Specifically, we suggest that it is the interaction between normative ideals and socio-economic power structures that fosters the development of the social conditions under which tech giants such as Google and Facebook can profit so tremendously from the commodification of personal communication in the first place. The ideals of a type of liberal individualism that is becoming increasingly one-sided from a normative perspective creates complicities with the structural dynamics of informational capitalism (Castells 1997), and these, in turn, promote those material-discursive practices of digital usage that are ultimately so incredibly privacy-invasive. This also has an impact on the privacy protection regimes that we analyze, which try to respond to these practices. In conclusion, we propose a concept of *privacy that is relational*, which we understand as a necessary complement to dominating concepts of *privacy as individual control*. Our concept of privacy as relational is based on empowerment and the social conditions enabling the realization of autonomy instead of presupposing autonomy.

Privacy in Platform Societies

In the late 1990s, Manuel Castells (1996) analyzed a shift from industrial societies to informational societies, which, according to his analysis, began in the 1970s. In Castells’s trilogy *The Information Age: Economy, Society, and Culture* (1996, 1997, 1998), he describes current societies as being centered around networks instead of individual actors and as working through a constant flow of information through technology. Within the last three decades, Castells’ (1996, 1997, 1998) analysis has been taken up by scholars from various disciplines, and it has been further developed and constantly adjusted to react to more recent technological innovations and the economic, societal, and political shifts that come along with them.

Here, we refer to the newly coined “platform concept” as one of these further developments of Castells’ “Information Age.” Platforms represent a specific form of network that has emerged during the last decade

and is currently developing towards monopolization.³ Focusing attention on platforms in this paper, which deals with the normative paradoxes of privacy regulation today, implies an understanding of platforms as powerful and influential enough to gradually turn the western democracies of our time into “platform societies.”

Srnicek (2017) first proposed the concept of “platform societies” and van Dijck, de Waal, and Poell (2018) further developed it.⁴ With the term platform, Srnicek (2017: 46–52) nails down a certain type of digital infrastructure that connects users and offers them tools for interaction, and is designed to collect, produce and accumulate data. Based on this definition, Srnicek examines the working logics of platforms in order to understand recent dynamics of oligarchization and centralization of power in regards to the “Big Five” tech companies (Alphabet, Facebook, Amazon, Apple, and Microsoft). Srnicek (2019) explains these dynamics as the result of a lack of alternatives that is created through a self-reinforcing effect produced by the sheer number of users paired with the accumulation of power gained through collecting more and more data.

In line with Srnicek’s analysis, van Dijck, de Waal, and Poell (2018) further argue that the shift created through “the platformization of society” is so fundamental that it can be diagnosed as paradigmatic. Platforms create new value regimes and economies; they expand their reach into every corner of society, and the most powerful platforms can even overrule the power of nation-states: they set the terms for how people communicate with each other, for how they interact, and for how they vote (van Dijck, de Waal, and Poell 2018: 24–25). The term platform surveillance more precisely focuses on how platforms transform all social practices and even subjectivities into “surveillant exchanges” whose coordination must be technologically mediated to make as much information as possible exploitable as data (Murakami Wood and Monahan 2019).

There are certainly many problems that come with these dynamics of platformization. Among them is the widely recognized fact that current approaches to privacy protection, which are mostly based on concepts of individual control and choice, fail to account for the immense power and influence of a few platforms whose data-driven agendas run counter to the protection of privacy. Despite acknowledging arguments against privacy, such as those raised by feminist and communitarian critiques (MacKinnon 1989; Pateman 1989; Etzioni 1999; Seignani 2016), we generally think that diminishing privacy protection in platform societies is a very concerning development. In order to make clear why we find it concerning, we will now reflect on the concept of privacy and the values that it is supposed to protect.

Debates about the challenges of legally enforced privacy protection vary across different liberal privacy regimes—for instance, they are different in the European Union and the United States (see Whitman [2004] for an account on this distinction). Here, however, we do not want to focus on national or regional differences because we are concerned with the general dynamics of platform societies. Platform societies are defined by the enormous influence of the “Big Five”: companies that are legally based in the US but operate worldwide. It was Manuel Castells (2008: 78) who suggested that with digitalization, the public sphere as the space for debate about public affairs has shifted from the national to the global. Following from this, instead of primarily being determined by local cultures and nation states, publics today are increasingly constructed around and shaped through the affordances provided by globally operating digital platforms that connect us across physical distances. In light of this development, privacy has increasingly become a matter of supranational concern (Hornung 2015). This is why, instead of focusing on regional differences, we want to provide an overview of common schemes and related shifts in scholarly and popular discourse on privacy.

³ Frequently addressed as the “Big Five”: Google, Amazon, Facebook, Apple, and Microsoft (van Dijck, de Waal, and Poell 2018: 2).

⁴ More recently, Murakami Wood and Monahan (2019) edited a special issue of *Surveillance & Society* on platform surveillance where they bring together reflections on platform societies and insights from surveillance studies.

There is a broad consensus today that privacy should not be seen as intrinsically valuable but valuable only because it facilitates self-determination. Functionally, privacy is related to individual autonomy. Privacy as a liberal value rests on the expectation of it making a positive contribution to self-affirmation and self-realization (Lever 2012: 17–29). The central idea is that we do not have to be accountable for certain issues in our lives because they are “nobody else’s business.” In the Anglo-Saxon tradition, privacy is traditionally understood as an individual defense right, with the aim of protecting people from interference from the government or unauthorized third parties (Warren and Brandeis 1890).

Following this conceptual path, privacy is primarily conceived negatively as exclusion and withdrawal: “shutting the world out” both literally and symbolically—i.e., closing the door but also liberating oneself from role expectations, traditions, etc. Even though privacy scholars such as Helen Nissenbaum (2009) have very rightly argued for a shift in the conceptualization of privacy from an individual to a social concept, this original conceptual idea endures in legal approaches to privacy, which define privacy as *control over access*. This can be access to a person’s space, an individual’s access to their own body, or access to decisions and information about the self.⁵ Control assumes that we can individually *possess* that which we are claiming control of. In this sense, privacy is linked to a specific liberal tradition of individualism that attributes not only material property but also intellectual property, such as thoughts, to the entitlement of individuals to “own” these types of properties as products of their labor.⁶

The control paradigm has been criticized widely within contemporary academic discourse on privacy (for an overview, see Helm and Eichenhofer 2019). Nevertheless, it is still the ruling paradigm in popular, legal, and economic discourse. A look at how Web-giants such as Facebook approach the issue makes this obvious. For example, Facebook’s (n.d.) “Privacy Basics” page says: “Learn how you are in control of your Facebook experience.”⁷ Here, Facebook very clearly adapts an understanding of privacy as control over personal information and suggests that this control is a matter of individual choice.

What happens to these ideas of individual control when data and communication become the economic target of a handful of increasingly powerful digital platforms? Algorithmic processing of data opens up endless possibilities to search for patterns and to create new combinations, correlations, and profiles. This offers enormous opportunities for optimization and profit but also challenges for the protection of privacy both in regards to the state and the private sector. In the last ten years, huge storage and evaluation capacities have been developed with which the control capacities of the democratic constitutional states of the world cannot keep pace, partly because future uses of data can hardly be foreseen (Mayer-Schönberger and Cukier 2013: 98–122). The new European General Data Protection Regulation (European Commission 2016) intends to overcome the vagueness of potential uses. Article V, paragraph 1, lays down a purpose limitation for the collection and further processing of personal data (European Commission 2016). However, in the case of an unforeseen “legitimate interest” on the part of the processor or a third party, data can, as is criticized, all too easily still be used for any purpose (see Roßnagel et al. 2019: 6).

At present, it is the huge economic interest in data that puts approaches to privacy protection as individual control in a precarious position (Solove 2008). What is more, users are significantly involved in the creation of this situation. They upload information about themselves and their lives online and they “like” and “retweet” other peoples’ information. Conversely, platform dynamics encourage a focus on a few providers and make privacy-sensitive but less-used providers such as the instant messenger “Signal” or the social media network “Diaspora” unattractive. In light of these socio-technical developments, the limitation of a liberal conception of privacy becomes very obvious. Although people would agree that they want protection

⁵ According to this interpretation, something is only “private” “if the individual is able to control access to this ‘something’” (Rössler 2015: 23). The traditional point of reference here is Alan Westin’s (1967: 7) definition: “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.”

⁶ For a discussion of the concept of “self-property,” see Locke ([1690] 2006); in relation to personal freedom, see Mill ([1859] 2001); and for a critical account of the concept, see Seignani (2016).

of their personal autonomy and of the integrity of social life, currently, everybody seems to be contributing to its erosion.

In such a world, tools for privacy protection that appeal to the responsibility of the individual are hardly likely to show significant effects. Julie Cohen (2008: 189), for instance, argues that current regimes of privacy protection fail because they only focus on informational aspects of transparency and surveillance, forgetting about the autonomy-impairing consequences of exposure—the most serious effect of constant surveillance. Exposure, according to Cohen (2008), has become the default in platform societies. It threatens the development of subjectivity through criticism and performance—in other words: autonomy. Privacy was traditionally meant to protect us from the threat of exposure.

Let's now take a more detailed look at the possible effects of two specific privacy protection measures that primarily operate on the idea of self-defense. How close are they to fulfilling the normative goals that they intend to reach?

Case Studies

Notice and Choice, Without Choice?

"Notice and Choice" is the current paradigm for consent online (Federal Trade Commission 2012). "The Notice" is a "presentation of terms, typically in a privacy policy or terms of use agreement. The Choice is an action signifying acceptance of the terms, typically clicking on an 'I agree' button, or simply using the website" (Sloan and Warner 2013). The approach aims to push individuals towards consenting to the privacy policies of Web providers but, in fact, encourages them to make an informed and free choice (Cate and Mayer-Schönberger 2013: 67). This mechanism therefore "is believed to be an effective means of respecting individuals as autonomous decision makers with rights of self-determination, including rights to make choices, take or avoid risks, express preferences, and, perhaps most importantly, resist exploitation" (Barocas and Nissenbaum 2014: 14).

However, what kind of choice do people really have when agreeing to the policies of Web providers? Is it genuinely free and informed? On the surface, privacy policies are readily presented to users for their critical review, but it is questionable whether such a critical review can actually take place. Given the fact that these texts often appear rather cryptic for the laity, it is easy to assume that they are written by lawyers to be understood only by members of their own profession (Bakos, Marotta-Wurgler, and Trossen 2014; McDonald and Cranor 2008). Thus, instead of critically reviewing privacy policies, most people seem to simply rely on the view that nothing unjust will be done with their data and that national privacy regulations will protect them from harm. Some scholars even suggest that privacy policies are elusive by design: "If websites and social media applications require individuals to share information to make money, it may be in their best interest to keep individuals in the dark about their use of personal data" (Madden et al. 2017: 118).

Critical accounts of "Notice and Choice" to date have primarily focused on the readability of the documents and the scope of their content: should the provider's responsibility end with informing subjects about data that are explicitly mined and sold, or should they also reveal whom they are selling it to, for what price, for what purpose, and what further information may be gleaned from these data (Sloan and Warner 2013)? Indeed, the *quality* of information is of utmost importance. Providers, however, are confronted with the difficulty of explaining that it is impossible to know in advance what further information might be derived from collected data and how this information might affect individuals.⁸ How then can these open-ended

⁸ What the mega-platform Facebook, for instance, discloses in this regard is more than vague: "We understand how people use our Services, and analyze and use the information we have to evaluate and improve our Services, research, develop, and test new services and features, and conduct troubleshooting activities" (WhatsApp 2018). This sentence might be readable, but it is not very precise. In fact, it could mean anything.

privacy policies be presented to data subjects as the basis for informed consent (Barocas and Nissenbaum 2014)?

In addition to this problem, there is the question of the *quality* of the choice itself. In platform societies, all other options apart from consenting to the privacy policies of a few powerful providers would be highly detrimental for the person making the decision. If an individual decided to opt-out, they might face higher fees when buying an item in store instead of purchasing it online; might not get a ticket or a good seat when purchasing last minute at the counter instead of in advance over the internet; and, worst of all, might not be able to participate in public debate, promote their ideas, skills, and knowledge, and enjoy mediated feelings of connectedness (Papacharissi 2016). All these options would be denied any person not consenting to the privacy policies of big Web providers.

In placing the burden to decide whether to opt-in to selling one's data on the "free" choice of users, the "Notice and Choice" regime helps platforms to distract attention from *their* responsibility.⁹ Choices taken by users may even be construed as a case against privacy: informed users appear not to care about their privacy and so they decide to opt-in (Xu, Katina, and Xi 2013). When looking at the decisions being made from a *relational* perspective—one that takes into account needs for recognition and social conditions for autonomy—it seems that the new data economy, with its monopolies, does not provide users with *real* choices. Instead, it confronts them with a decision between being excluded from social participation, being turned into a lone-wolf, and being marginalized or agreeing to sell one's data (Zimmermann 1999). When "Notice and Choice" does not comprise of any kind of *genuine* choice, in the sense of socially equally respectable alternatives, it is corrupting the idea of self-determination through choice and then promoting it.

Therefore, in platform societies where mining and analyzing data has become the leading business model and where a few companies accumulate more and more data power, the normative objectives of autonomy and resistance that underpin the clause for "Notice and Choice" are being taken *ad absurdum*. Instead, the prevailing "Notice and Choice" regime that operates without reasonable choice seems to serve as an instrument for platform providers. Individually, users cannot solve the dilemma between their needs to participate, connect, and be heard and their need to protect their privacy (Helm 2018). They are, therefore, forced into selling these data. The decision to consent, surrendering one's privacy, should therefore be understood less as the result of a free and autonomous choice and more as a choice that is borne out of constraint. Failure to take this constraint into account provides a basis for the interpretation that people do not value their privacy. This then turns "Notice and Choice" into a tool to be used against the case of privacy rather to promote it, which was the original purpose of this mechanism (Cate and Mayer-Schönberger 2013).

Privacy Literacy: Responsibilities and Their Limits

Another prominent endeavor intended to meet the challenges that digitalization poses to established values such as participation, autonomy, and agency, is the idea of privacy literacy. The normative goal of the wide variety of privacy literacy programs is to empower users to protect themselves, teaching them certain skills and imparting knowledge about how the internet works, how their data are being processed and analyzed, and how to use privacy-enhancing technologies (PETs) such as encryption. The term privacy literacy is a subcategory of the more general and well-known concept of media literacy, particularly digital literacy (Livingstone 2004).¹⁰ Digital literacy encompasses all educational programs that refer to the vast array of "technical, cognitive, and sociological skills that individuals need in order to perform tasks and solve problems in the digital environment" (Eshet-Alkalai 2004).

⁹ "Giving individuals notice and choice may simply perpetuate the growing gap between consumer 'haves' and 'have-nots' because the least sophisticated consumers remain least likely to protect themselves" (Schmitz 2014: 1463).

¹⁰ Because of the diversity of existing approaches, Lankshear and Knobel (2008) suggest that it might be better to refer to "literacies" in the plural.

At first glance, the notion seems tremendously promising in terms of increasing the agency and autonomy of internet users (Trepte et al. 2015). Educating, and thereby empowering, citizens to critically engage with new information and communication technologies (ICTs) is without question a very worthy goal (Martens and Hobbs 2015). Nevertheless, the underlying theoretical assumptions, as well as the aims and scope of privacy literacy, need to be carefully reviewed. This is because—as is continuously highlighted in recent studies pointing out the inscribed biases of algorithmic decision-making—there are all kinds of possible types of discrimination and manipulation that can result from platform surveillance and data analytics that are taking place at a systemic level, beyond the reach of (well-educated) individuals (Murakami Wood and Monahan 2019; boyd, Levy, and Marwick 2014; Bird et al. 2016; Barocas and Levy 2018; Levy and Barocas 2017; Madden et al. 2017; Bridges 2018; Eubanks 2018).

Let's take a look at how privacy literacy might affect patterns of usage and thus privacy protection. To do so, we imagine a young woman, Sophie, who lives in a liberal democracy and has recently participated in a privacy literacy workshop. Having learned a lot about the functioning of platform surveillance and about privacy self-defense tactics, Sophie is now enthusiastic to transfer what she has learned into practice.

When reviewing the privacy policies of her smartphone applications, Sophie is relieved to read that the instant messenger WhatsApp has implemented end-to-end-encryption by default (WhatsApp 2020a). She is stunned, however, by the amount of metadata that WhatsApp is collecting, as well as by the amount and sort of information that it is drawing from her smartphone (WhatsApp 2020b). When installing the app, Sophie had lightheartedly agreed when it asked whether she was “ok” with the app accessing information from her phone. Now, she is troubled. This feeling increases when she realizes that Facebook owns WhatsApp and that all of the data she is sharing on WhatsApp can and will be used by Facebook.¹¹ A few years ago, she had deactivated her Facebook account because she had found it too “addictive,” only to now realize that she is still taking the “drug.” It had simply changed its shape (Hiltzik 2019). She also feels guilty because she knows that some of her friends are very sensitive about their privacy. She now realizes that it was her that provided Facebook with information about these friends when she had allowed Facebook to access information from her phone via WhatsApp.

Sophie tries to adjust her privacy settings but soon realizes that when Facebook says on its “Privacy Basics” page that “you’re in charge” and that you can “manage your privacy” (Facebook n.d.), it is referring exclusively to what other *users* may see and know. What is *not negotiable* is the sort and amount of data that Facebook collects, stores, analyzes, and mines as soon as one wishes to use its services. There is no alternative payment option available other than to pay with your data. Sophie therefore decides to deinstall WhatsApp from her phone. A week later, she realizes that friends and colleagues are scheduling appointments without her approval. They also keep sharing and commenting on pictures and events that include her, except now she is missing out on the opportunity to reply to these comments and pictures. The phenomenon of privacy protection increasingly becoming an interdependent matter has been dubbed “network privacy” (boyd and Marwick 2014; boyd, Levy, and Marwick 2014: 43–57).

What this case is meant to illustrate is that when doing it individually, privacy literacy does little to protect people from privacy intrusion. Academic discourse on privacy literacy is partially aware of the challenges of developing and establishing good and effective media and privacy literacy programs (Hobbs 1998). Scholars, such as Sonja Livingstone (2004), have already hinted at the “governmental” dynamics that literacy programs might develop when they’re addressing people as isolated individuals instead of as “networked selves” (Cohen 2012). Even though many literacy regimes have been reviewed critically in this regard, people still refer to them as a possibility for a healthier, safer, and more humane handling of digital technologies (boyd 2018). It is precisely because of the high hopes many people attach to ideas of privacy

¹¹ Currently, Facebook is reportedly planning to integrate its messaging services WhatsApp, Instagram, and Facebook into one mega-platform. Although claiming to ensure high levels of protection against outside intrusion (e.g., via end-to-end encryption), this move gives Facebook huge additional power with regard to the data—particularly meta-data—of (even more) users inside the “circle.”

literacy that we need to review the respective programs critically—not only in terms of their limitations but also in terms of the potential harms that may derive from not *acknowledging* these limitations.

Not acknowledging the limitations of current privacy literacy programs could increase their problematic effects. This happens, for instance, when the idea of privacy literacy is combined with neoliberal regimes of responsibilization. Such models suggest that “if an individual’s privacy is violated, it is because she did not protect it adequately. This places the fault on the individual rather than the person or organization that violated her privacy” (Madden et. al 2017: 118). Regimes of responsibilization can further be considered problematic because they mistakenly perceive the ideal of agency through education as a catchall solution, even in situations where the problem is not so much a lack of individual literacy as it is a structural problem that refers to power asymmetries created through exposure, surveillance, and the asymmetric distribution of data power (Cohen 2008). Such structural problems, however, can’t be solved on an individual basis but need to be addressed by higher authorities. Here, privacy literacy can do only so much and needs to be combined with other forms of privacy regulation in order to safeguard autonomy, enable resistance, and foster agency.

How Do We Make Sense of These Paradoxical Conversions?

How can we make sense of the ambivalent, if not paradoxical, outcomes of these two privacy protection measures? To help us understand the more complex structural dynamics that are at play here, we will now turn to the more broadly aligned social theoretical framework of “normative paradoxes” elaborated by scholars at the Frankfurt Institute for Social Research (Honneth and Sutterlüty 2011; Honneth and Sutterlüty 2012). The analytical framework of “normative paradoxes” provides us with a reconstructive interpretation of societal developments, where a normative promise is converted into its opposite in the course of its successful institutionalization or parallel socio-economic developments.

The approach takes a critical stance toward popular critical social theory concepts (such as Habermas’ [1963] “colonization thesis”) to the extent that they traditionally counterpose the capitalist market economy’s exploitative interests with a rationalization of the lifeworld. The boundaries between lifeworld and system, culture and economy, and, we could also add here, between the private and the public are becoming increasingly blurred. Often, one and the same norm can be used to justify both emancipatory behavior and actions striving to increase authority and control. Normative principles continue to have performative actuality (*performative Aktualität*), but, beneath the surface, have lost their emancipatory meaning or have been altered so dramatically that, in many contexts, they have become nothing more than concepts legitimizing a new stage of capitalist expansion (Honneth and Sutterlüty 2011: 69).

The theory of normative paradoxes developed by Axel Honneth and Ferdinand Sutterlüty (2011) comprises various different types of paradoxical conversion. Two are especially important for our context. The first type is where the idea underpinning a societal development itself increasingly becomes distorted over the course of its realization. The second type comprises the identification of parallel societal developments, which contribute to successfully institutionalized principles becoming channels of a disempowering form of integration. So how can we now apply these ideas to the issue of privacy? To what extent can privacy be considered an initially emancipatory idea that has forfeited its emancipatory power?¹² Following the liberal tradition, the concept of privacy has predominantly been developed along the lines of a “control paradigm,” and it is this control paradigm that is also implied in the two cases investigated above. Both cases—“Notice and Choice” and privacy literacy—rely on the idea of privacy as self-defense. But instead of promoting and protecting autonomy through privacy, they contribute to a loss of confidence in privacy.

¹² It is impossible to provide a comprehensive normative reconstruction of the value of privacy here. However, it should at least be mentioned that, as an emancipatory idea, privacy is linked to a specific modern understanding of freedom, which itself is also inherently related to traditions of critique (see Seubert and Becker 2019).

Both types of paradoxical conversion are important here: the distortion of the value itself as well as the dynamics of parallel developments. In the first variant, the idea of autonomy (to which the concept of privacy is functionally related) is attributed solely to a negative conception of freedom, which tends to distort the concept because it becomes totally abstracted from the social conditions of its realization. Moreover, the definition of privacy as individual control over information and access is an inadequate basis for countering its further commodification. This interpretation suggests that privacy is only something that an individual may or may not choose to possess, and the logical consequence is that it has a price and can be sold. A liberal, property-based understanding therefore prepares the ground for privacy to be comprehensively converted into a commodity with market value—where data are invested as an economic resource.

This leads us to the second variant. Here, unintended outcomes or even paradoxical conversions are supposed to appear because over the course of the successful institutionalization of privacy protection regimes, these endeavors have become incorporated into parallel processes of marketization and commodification encompassed by platform capitalism (Honneth and Sutterlüty 2012: 60–61). While the normative idea of privacy is still “performatively actualized,” it is in fact being hollowed out and is increasingly losing its emancipatory meaning. The more privacy is publicly invoked as a societal value, the more it becomes a tool for the expansion and legitimation of a data economy that systematically includes and is built upon privacy violations rather than for contributing to processes fostering personal freedom. Privacy legislation, framed in liberalist terms of individual control, is therefore likely to become a governmental mechanism, overburdening individuals rather than allowing the social conditions for personal and social freedom to flourish (Flyverbom, Madsen, and Rasche 2017). Despite its promises of liberation, this form of privacy is likely to perpetuate neoliberal regimes of responsabilization—an outcome that diverges dramatically from the normative goal initially intended.

Toward a Relational Understanding of Privacy as a Social Good

In light of the serious weaknesses of current approaches to privacy protection and their tendency to produce results that divert from the initially intended outcome, many commentators have argued that we should let go of our concentration on privacy. Privacy just no longer seems to do justice to the systemic threats of new forms of surveillance (Lyon 2015). Instead, other approaches are being suggested such as data justice, data activism, or algorithmic accountability (Dencik, Hintz, and Cable 2016; Taylor 2017; Caplan et al. 2018; Diakopulus 2016; Milan and van der Velden 2016). While we also consider these other approaches to be promising, we think that it might still be worthwhile to continue exploring the notion of privacy on the condition that it is reformulated in a way that is better aligned with the challenges we are facing today. These challenges not only arise from nation-states reaching their limits due to the speed and scope of technological innovation. They also include huge power asymmetries stemming from a digital divide between five powerful platforms, which have the power to collect, store, and analyze data by using their respective infrastructures and writing their respective algorithms, and those who lack that power and are instead enmeshed in a web of interdependent profiling and uncontrollable data flows (boyd and Crawford 2012; Dalton, Taylor, and Kitchin 2016).

In order to establish a conception of privacy that is capable of meeting the challenges posed by these new conditions, we need to reformulate our underlying understanding of autonomy so that it does justice to the datafied, divided, and networked reality of today’s social world. Then we need to rethink privacy on the basis of this alternative understanding. To do so, we start with *a relational understanding of autonomy*, which takes into account the social conditions necessary to develop autonomy. Approaching privacy based on such a relational understanding of autonomy radically shifts our focus. Instead of concentrating primarily on privacy’s function as a means to withdraw from society, privacy is now to be assigned a much more general and, at the same time, more conditional function: it ought to be protected if—and *only* if—it serves to protect and cultivate the integrity of autonomy-conducive contexts. The contexts where privacy is to be considered relevant thus not only include spheres valued for their intimacy, such as those related to family life, but also professional, artistic, medical, and even political domains.

The logical consequence of such a shift requires a redefinition of privacy. Instead of defining privacy solely in terms of the individual's capacity to draw informational boundaries and to restrict access, we now require a broader definition of privacy as the intersubjective negotiation of boundaries and informational flows (Altman 1975). Adopting this approach to defining privacy enables us to go beyond a possessive individualistic understanding of the concept, as it emphasizes an interpretation of privacy as a relational good whose achievement and protection should be treated as a collective challenge. Therefore, privacy should no longer be considered a communicative one-way street but a social practice serving to protect a variety of autonomy-conducive communicative contexts.

Another aspect refers to the relevance of privacy as the necessary basis for the creation and cultivation of a genuinely democratic public. Manuel Castells (2008) claims that debates on public affairs are increasingly shifting from the national to the global. We add that, as a result of this globalization of the public, debates are increasingly dependent on the mediation of internationally operating and privately owned platforms, which rely on an economic interest in data and (personal and political) communication. In light of this development, we need to rethink the relationship between the public and the private. We need to abandon the traditional idea of conceptualizing the private and the public as distinct spheres (the political versus the personal) and instead think of them as interdependent. Understood as interdependent concepts, it then becomes very clear that every crisis of privacy will necessarily go hand in hand with a crisis of the public and, hence, of democratic life.

Given these considerations, it is not at all surprising that some of the most relevant political struggles within liberal democratic societies are currently linked to the matter of privacy. Here, it is not primarily the claim of individuals who want to be left alone that dominates these struggles (Warren and Brandeis 1890). What prevails instead is the claim of (political) collectives that struggle to achieve communicative autonomy by asserting their right to anonymity and privacy (Electronic Frontier Foundation 2020; Coleman 2014: 401–426). In this context, privacy is being practiced and treated as a condition for political activism and free debate on public affairs rather than as a counterpart to the political, as was suggested by the traditional liberal understanding.

If we look at these political struggles revolving around a digital crisis of privacy through the lens of a performative perspective, it becomes quite obvious that it is no longer useful to conceptualize privacy as a counterpart to the public, the political, and the democratic. According to scholars such as Colin Bennet (2014) and Eigin Isin and Evelyn Ruppert (2015), quite the opposite is true. They identify precisely these discourses that revolve around matters of privacy, data protection, information flow, surveillance, exposure, and anonymity as those through which a new form of citizenship is being performatively enacted through new media—a form of citizenship referred to by Isin and Ruppert (2015: 43, 65–71) as *digital* citizenship (Bennet 2014). According to this performative view, it is during the course of the crisis of privacy and its related politicization (at the latest) that we see privacy transformed from a matter of individual choice and responsibility into a matter of political contestation. Individuals should not be overburdened with the responsibility for resolving this issue. Instead, it must be approached and addressed as a common democratic challenge of our time.

Concluding Remarks

Privacy is often referred to as a powerful liberal concept. The right to privacy is meant to protect us from intrusion, manipulation, harassment, exploitation, and the like. Over the last few decades, however, an increasingly one-sided form of liberal individualism has merged with the structural dynamics of platform capitalism. These dynamics depend on masses of people disclosing personal data on digital platforms because they want and need to participate, connect, and profit from the opportunities these new communicative infrastructures offer. The data they disclose are not primarily analyzed individually but instead used for mass analysis—creating types, categories, and profiles of people. The methodological individualism of today's privacy regulation fails to adhere to the systemic dimensions behind the functioning

of platform societies, systemic dimensions that also result in surveillance, exposure, and a lack of privacy protection that threaten to undermine our autonomy.

Reacting to these threats, policymakers create new programs and work on reforms, such as privacy literacy and “Notice and Choice,” with the objective of identifying constructive responses to a digital crisis of privacy. Privacy advocacy, scholarship, and activism, however, continuously point to the limitations of these reformative endeavors. We go one step further by analyzing effects that show ambivalent and sometimes even paradoxical consequences. By referring to the framework of “normative paradoxes,” we suggest that these paradoxical consequences are caused by two factors:

1. The underlying understanding of what privacy is meant to protect. The underlying idea of autonomy (to which the concept of privacy is functionally related) is attributed solely to a negative conception of freedom. This tends to distort the concept because it becomes totally abstracted from the social conditions of its realization (relational autonomy).
2. An over-reliance on privacy protection as self-defense. While the normative idea of privacy is still “performatively actualized” in regimes such as “Notice and Choice,” it is in fact being hollowed out and is increasingly losing its emancipatory meaning. The more privacy is publicly invoked as a societal value, but without appropriate measures to protect this value, the more it becomes a tool for the expansion and legitimation of a data economy that systematically includes and is built upon privacy violations rather than for contributing to processes fostering autonomy.

Instead of understanding privacy relationally as a practice vital for people to cultivate social contexts that foster autonomy, ensuring individual control over personal data is still widely perceived as the primary means of privacy protection—as well as the means for reformative endeavors (Cate and Mayer-Schönberger 2013: 68). Based on this narrow understanding, the responsibility of privacy protection is, for the most part, placed on the individual. Individuals, however, are completely overburdened by the task. Any attempt to cover a serious lack of privacy protection must, first and foremost, break from the possessive individualistic understanding of privacy because this understanding is part of the very same logic which threatens to violate the integrity of many autonomy-conducive social contexts. Any method of enforcing such an understanding of privacy is therefore bound to turn into a normative paradox.

As an alternative, we suggest basing future attempts at reforming privacy regulation on an understanding of privacy based on a relational conception of autonomy. Such understanding takes into account the social conditions necessary for the development of autonomy. Only based on this understanding can the challenges faced by platformization be adequately addressed. These challenges cannot be tackled by important, yet individualistic, measures such as promoting privacy literacy and “Notice and Choice” alone. In order to reach their normative goals, these measures need to be complemented by privacy protection measures that approach the issue as a supranational democratic challenge.

References

- Altman, Irwin. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey, CA: Brooks/Cole.
- Bakos, Yanis, Florencia Marotta-Wurgler, and David Trossen. 2014. Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts. *Journal of Legal Studies* 43 (1).
- Barocas, Solon, and Karen Levy. 2018. Refractive Surveillance: Monitoring Customers to Manage Workers. *International Journal of Communication* 12: 1166–88.
- Barocas, Solon, and Helen Nissenbaum. 2014. Big Data’s End Run around Anonymity and Consent. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, 44–75. New York, NY: Boulder.
- Bennett, Colin. 2014. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.
- Bird, Sarah, Solon Barocas, Kate Crawford, Fernando Diaz, and Hanna Wallach. 2016. Exploring or Exploiting? Social and Ethical Implications of Autonomous Experimentation in AI. Fairness, Accountability, and Transparency in Machine Learning, workshop. New York, NY: New York University Press.

- boyd, danah. 2018. You Think You Want Media Literacy... Do You? *Data & Society: Points*, March 9. <https://points.datasociety.net/you-think-you-want-media-literacy-do-you-7cad6af18ec2> [accessed January 20, 2019].
- boyd, danah, and Kate Crawford. 2012. Critical Questions for Big Data. *Information, Communication and Society* 15 (5): 662–79.
- boyd, danah, and Alice Marwick. 2014. Networked Privacy: How Teenagers Negotiate Context in Social media. *New Media & Society* 16 (7): 1051–67.
- boyd, danah, Karen Levy, and Alice Marwick. 2014. The Networked Nature of Algorithmic Discrimination. In *Data & Discrimination: Collected Essays*, edited by Seeta P. Gangadharan and Virginia Eubanks, 43–57. Washington, DC: Open Technology Institute.
- Bridges, Khiara. 2018. *The Poverty of Privacy Rights*. Stanford, CA: Stanford University Press.
- Busch, Andreas. 2015. Privacy, Technology, and Regulation: Why One Size is Unlikely to Fit All. In *Social Dimensions of Privacy – Interdisciplinary Perspectives*, edited by Beate Rössler and Dorota Mokrosinska, 303–323. Cambridge, UK: Cambridge University Press.
- Caplan, Robyn, Joan Donovan, Lauren Hanson, and Joana Matthews. 2018. Algorithmic Accountability: A Primer. *Data & Society*, April 18. <https://datasociety.net/output/algorithmic-accountability-a-primer/> [accessed December 20, 2018].
- Castells, Manuel. 1996. *The Information Age: Economy, Society, and Culture, Volume 1: The Rise of the Network Society*. Oxford, UK: Blackwell Publishers.
- . 1997. *The Information Age: Economy, Society, and Culture, Volume 2: The Power of Identity*. Oxford, UK: Blackwell Publishers.
- . 1998. *The Information Age: Economy, Society, and Culture, Volume 3: End of Millennium*. Oxford, UK: Blackwell Publishers.
- . 2008. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. *The Annals of the American Academy of Political and Social Science* 616 (1): 78–93.
- Cate, Fred H., and Victor Mayer-Schönberger. 2013. Notice and Consent in a World of Big Data. *International Data Privacy Law* 3 (2): 67–73.
- Cohen, Julie. 2008. Privacy, Visibility, Transparency, and Exposure. *University of Chicago Law Review* 75: 181–201.
- . 2012. *Configuring the Networked Self: Law, Code and the Play of Everyday Practice*. New Haven, CT: Yale University Press.
- Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York, NY: Verso Books.
- Dalton, Craig M., Linnet Taylor, and Jim Thatcher. 2016. Critical Data Studies: A Dialog on Data and Space. *Big Data & Society* 3 (1): 1–9.
- Dencik, Lina, Arne Hintz, and Jonathan Cable. 2016. Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism. *Big Data & Society* 2 (2): 1–12.
- Diakopoulos, Nick. 2016. Accountability in Algorithmic Decision Making. *Communications of the ACM* 59 (2): 56–62.
- Electronic Frontier Foundation. 2020. Anonymity. <https://www.eff.org/issues/anonymity> [accessed May 7, 2020].
- Eshet-Alkalai, Yoram. 2004. Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era. *Journal of Educational Multimedia & Hypermedia* 13 (1): 93–106.
- Etzioni, Amitai. 1999. *The Limits of Privacy*. New York, NY: Basic Books.
- Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St Martin's Press.
- European Commission. 2016. Data Protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [accessed May 7, 2020].
- Facebook. n.d. Privacy Basics. <https://www.facebook.com/about/basics> [accessed May 7, 2020].
- Federal Trade Commission. 2012. FTC Issues Final Commission Report on Protecting Consumer Privacy: Agency Calls on Companies to Adopt Best Privacy Practices. The Federal Trade Commission, March 26. <https://perma.cc/7PM6-ZV6K> [accessed May 7, 2020].
- Flyverbom, Mikkel, Anders K. Madsen, and Andreas Rasche. 2017. Big Data as Governmentality in International Development: Digital Traces, Algorithms, and Altered Visibilities. *The Information Society* 33 (1): 35–42.
- Fried, Charles. 2009. Privacy: A Moral Analysis. In *Philosophical Dimensions of Privacy*, edited by Ferdinand D. Schoeman, 203–22. Cambridge, UK: Cambridge University Press.
- Gusy, Christoph, Johannes Eichenhofer, and Laura Schulte. 2016. e-privacy. Von der Digitalisierung der Kommunikation zur Digitalisierung der Privatsphäre. *Jahrbuch des Öffentlichen Rechts der Gegenwart* 64: 385–409.
- Habermas, Jürgen. 1963. *Strukturwandel der Öffentlichkeit*. Frankfurt am Main, DE: Suhrkamp.
- Helm, Paula. 2018. Treating Sensitive Topics Online: A Privacy Dilemma. *Ethics and Information Technology* 20 (4): 303–13.
- Helm, Paula, and Johannes Eichenhofer. 2019. Reflektionen zu einem social turn in den Privacy Studies. In *Privatheit und Digitalisierung*, edited by Martin Henning, Christian Aldenhoff, Lukas Edeler, Martin Hennig, Jacob Kelsch, Lea Raabe, and Felix Solaba, 139–166. Bielefeld, DE: Transcript.
- Hiltzik, Michael. 2019. Ex-Google Manager Leads a Drive to Rein in the Pernicious Impact of Social Media. *The Los Angeles Times*, May 10. <https://www.latimes.com/business/hiltzik/la-fi-hiltzik-tristan-tech-20190510-story.html> [accessed May 7, 2020].
- Hobbs, Rene. 1998. The Seven Great Debates in the Media Literacy Movement. *Journal of Communication* 48: 6–32.
- Honneth, Axel, and Ferdinand Sutterlüty. 2012. Normative Paradoxien der Gegenwart. In *Transnationale Vergesellschaftungen*, edited by Hans-Georg Söeffner, 897–909. Wiesbaden, DE: Springer.
- . 2011. Normative Paradoxien der Gegenwart. Ein Forschungsprogramm. *Neue Zeitschrift für Sozialforschung* 8 (1): 67–85.
- Hornung, Gerrit. 2015. Informationelle Selbstbestimmung oder Privatheit? Zu den semantischen und normativen Unterschieden verschiedener Konzepte des Persönlichkeitsschutzes im „digitalen“ Zeitalter. Presented at the Konferenz des forums privatheit

- „Die Zukunft der informationellen Selbstbestimmung,” November 2015. Berlin, Germany. https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/veranstaltungen/veranstaltungsdokumente/2015-11-26u27_dokumentation_zukunft-der-informationellen-selbstbestimmung/1.1.c-Hornung-Gerrit-Vortrag-Berlin-151126.pdf [accessed May 7, 2020].
- Isin, Eigin, and Evelyn Ruppert. 2015. *Being Digital Citizens*. London, UK: Roman International.
- Lankshear, Colin, and Michele Knobel. 2008. *Digital Literacies: Concepts, Policies and Practices*. New York, NY: Peter Lang Publishing.
- Lever, Annabelle. 2012. *On Privacy*. London, UK: Routledge.
- Levy, Karen, and Solon Barocas. 2017. Designing Against Discrimination in Online Markets. *Berkeley Technology Law Journal* 32 (3): 1183–237.
- Livingstone, Sonja. 2004. Media Literacy and the Challenge of New Information and Communication Technologies. *The Communication Review* 7: 3–14.
- Locke, John. (1690) 2006. *Two Treatises on Government*. Farmington Hill, MI: Thomson Gale.
- Lyon, David. 2015. *Surveillance after Snowden*. Malden, MA: Polity Press.
- MacKinnon, Catharine A. 1989. *Toward a Feminist Theory of the State*. Cambridge, UK: Cambridge University Press.
- Madden, Mary, Michele Gilman, Karen Levy, and Alice Marwick. 2017. Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review* 95: 53–118.
- Martens, Hana, and Renee Hobbs. 2015. How Media Literacy Supports Civic Engagement in a Digital Age. *Atlantic Journal of Communication* 23 (2): 120–137.
- Mayer-Schönberger, Victor, and Kenneth Cukier. 2013. *Big Data. A Revolution that will Transform How We Live, Work, and Think*. New York, NY: Houghton Mifflin Harcourt Publishing Company.
- McDonald, Aleecia M., and Lorrie F. Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (3): 540–65.
- Milan, Stefania, and Lonneke van der Velden. 2016. The Alternative Epistemologies of Data Activism. *Digital Culture & Society* 2 (2): 57–74.
- Mill, John S. (1859) 2001. *On Liberty*. Blacksburg, VA: Virginia Tech University Press.
- Murakami Wood, David, and Torin Monahan. 2019. Editorial: Platform Surveillance. *Surveillance and Society* 17 (1/2): 1–6.
- Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford, CT: Stanford University Press.
- Papacharissi, Zizi. 2016. Affective Publics and Structures of Storytelling: Sentiment, Events and Mediality. *Information, Communication & Society* 19 (3): 307–324.
- Pateman, Carole. 1989. Feminist Critiques of the Public/Private Dichotomy. In *The Disorder of Women. Democracy, Feminism and Political Theory*, edited by Carole Pateman, 118–140. Stanford, CT: Stanford University Press.
- Reiman, Jeffrey. 1995. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara High Technology Law Journal* 11 (27): 27–44.
- Roßnagel, Alexander, Christian Geminn, Maxi Nebel, and Tamer Bile. 2019. Evaluation der Datenschutz-Grundverordnung. Policy Paper des Forums Privatheit und selbstbestimmtes Leben in der digitalen Welt. Karlsruhe, DE: Forum Privatheit.
- Rössler, Beate. 2015. Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy. In *Social Dimensions of Privacy*, edited by Beate Rössler and Dorota Mokrosinska, 141–161. Cambridge, UK: Cambridge University Press.
- Schmitz, Amy J. 2014. Secret Consumer Scores and Segmentations: Separating Consumer “Haves” from “Have-Nots.” *2014 Michigan State Law Review*: 1411–26.
- Seubert, Seubert, and Carlos Becker. 2019. The Culture Industry Revisited: Socio-Critical Reflection on the Value of Privacy. *Philosophy and Social Criticism* 45 (8): 930–947.
- Sevignani, Sebastian. 2016. *Privacy and Capitalism in the Age of Social Media*. New York, NY: Routledge.
- Sloan, Robert H., and Richard Warner. 2013. Beyond Notice and Choice: Privacy, Norms, and Consent. *J. High Tech. L.*: 370–412.
- Solove, Daniel. 2008. The End of Privacy? *Scientific American* 299 (3): 100–106.
- Sprenger, Polly. 1999. Sun on Privacy: “Get Over It.” *Wired*, January 26. <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> [accessed May 7, 2020].
- Srnicek, Nick. 2017. *Platform Capitalism*. Malden, MA: Polity.
- . 2019. Platform Monopolies and the Political Economy of AI. In *Economies for the Many*, edited by John McDonnell, 152–163. London, UK: Verso.
- Taylor, Linnet. 2017. What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally. SSRN, June 28. <https://ssrn.com/abstract=2918779> [accessed September 10, 2018].
- Trepte, Sabine, Doris Teutsch, Philip Masur, Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. 2015. Do People Know About Privacy and Data Protection Strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In *Reforming European Data Protection Law*, edited by Serge Gutwirth, Ronald Leenes, and Paul de Hert, 333–65. Dordrecht, NL: Springer.
- van Dijck, José, Martijn Waal, and Thomas Poell. 2018. *The Platform Society: Public Values in a Connective World*. Oxford, UK: Oxford University Press.
- Warren, Samuel D., and Louis D. Brandeis. 1890. The Right to Privacy. *Harvard Law Review* IV (5): 193–220.
- Westin, Allan. 1967. *Privacy and Freedom*. New York, NY: Atheneum.
- WhatsApp. 2018. WhatsApp Terms of Service. April 24. <https://www.whatsapp.com/legal?eca=1-privacy-policy-information-we-collect> [accessed August 20, 2019].
- . 2020a. End-to-End Encryption. <https://faq.whatsapp.com/en/android/28030015/> [accessed May 7, 2020].

- . 2020b. Usage of Your Phone Number and Address Book. <https://faq.whatsapp.com/en/iphone/20971813> [accessed May 7, 2020].
- Whitman, James Q. 2004. The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal* 113: 1151–1221.
- Xu Feng, Michael Katina, and Chen Xi. 2013. Factors Affecting Privacy Disclosure on Social Network Sites: An Integrated Model. *Electronic Commerce Research* 13 (2): 151–168.
- Zimmermann, Philip. 1999. Why I wrote PGP. Phil Zimmermann (blog), June. <https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html> [accessed August 12, 2019].