COGITATIO

Article

Localizing the Politics of Privacy in Communication and Media Research

Johanna E. Möller * and Leyla Dogruel

Department of Communication, Johannes Gutenberg University Mainz, 55128 Mainz, Germany;
E-Mails: johanna.moeller@uni-mainz.de (J.E.M.), dogruel@uni-mainz.de (L.D.)

* Corresponding author

Abstract
While previous communication and media research has largely focused on either studying privacy as personal boundary management or made efforts to investigate the structural (legal or economic) condition of privacy, we observe an emergent body of research on the political underpinnings of privacy linking both aspects. A pronounced understanding of the politics of privacy is however lacking. In this contribution, we set out to push this forward by mapping four communication and media perspectives on the political implications of privacy. In order to do so, we recur on Barry's (2002) distinction of the political and the politics and outline linkages between individual and structural dimensions of privacy. Finally, we argue that the media practice perspective is well suited to offer an analytical tool for the study of the multiple aspects of privacy in a political context.

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

1. Introduction

Privacy has a political dimension, which communication and media scholars increasingly address (Katzenbach & Bächle, 2019; Matzner & Ochs, 2019). It offers a conceptual framework for embracing both the ambiguous complexity of managing information-flow boundaries and related agency and civic freedom in an era in which communication and media technologies are driving massive societal transformations. Snowden's revelations about massive transnational surveillance operations have made us all aware of privacy-infringing technologies and practices related to political interventions (Bauman et al., 2014). This has resulted in new journalistic encryption practices and citizens' increased awareness of data security. More recent debates emerging during the coronavirus pandemic emphasize the other side of political privacy implications. Numerous voices underscore the need to collect and analyze personal (instead of anonymized and collective) movement data to monitor compliance with quarantine rules. At the same time, other voices question the usefulness of such political measures and express doubt that they will be reversed when the period of immediate danger is over (Singer & Sang-Hun, 2020). In this regard, political decision-making varies widely, has consequences for limiting the private sphere, and eventually implies a shift of power in favor of governments and not citizens. While China and South Korea fight the coronavirus using individual data tracking and combining video surveillance and face recognition, German experts publicly justify and explain their restricted data analysis practices that are based on anonymized mass data.

Beyond everyday examples, the academic literature points to the political implications of privacy. While citizens might aim to (re)gain control of their data, digital platforms use public discourse to downplay the political

implications of their activities and strive to mask their massive invasions of privacy (Gillespie, 2010). Recent publications address related privacy challenges in the realms of journalism (Lokot, 2018), digital citizenship (Hintz, Dencik, & Wahl-Jorgensen, 2019), and agency (Baruh & Popescu, 2017). Some defend broader concepts, such as data protection (Bellanova, 2017, p. 329) or data justice (Dencik, Hintz, Redden, & Treré, 2019, p. 874), to embrace the pitfalls of information management in digital environments.

Researchers discussing these diverse political implications of privacy relate them to the scattered and interdisciplinary field of privacy research (Bräunlich et al., 2020). So far, communication and media research in this field predominantly focused on individual-centered psychological approaches, considering the paradoxes emerging from balancing individual privacy literacies and social embeddedness. Increasing attention is recently though being given to the structural implications of privacy, such as concerns regarding the utilization of data to manipulate users (Susser, Roessler, & Nissenbaum, 2019) and the unreflected uses of communication channels, including WhatsApp, to transfer sensitive information related, for example, to one's health (Rose, Littleboy, Bruggeman, & Rao, 2018). This way, insights from information science (Nissenbaum, 2010), economics (Martin & Murphy, 2017), and legal studies (Regan, 2016) need to be more thoroughly integrated into communication and media studies' analysis of privacy.

In this emerging field, the question of what communication and media researchers actually mean when addressing the political implications of privacy remains often unclear. In contrast to the view that there is a need for new definitions of privacy vis-à-vis politics (Matzner & Ochs, 2019), we follow Nissenbaum (2019, p. 223), who holds that despite massive datafication processes, no development concerning privacy has been disruptive. Our plea is to consider what we actually mean by 'the political' and 'politics' with regard to the reassessment of contemporary uses of privacy. In this article, we seek to develop a roadmap to distinguish communication and media-related privacy research and their political implications. In particular, we first review existing communication and media research on privacy, both individual strategies and structural preconditions. Second, we develop a concept of what the political could mean. Finally, we demonstrate how existing research on the political implications of privacy can be clustered around four research perspectives.

2. Communication and Media Privacy Research

Given the interdisciplinary nature of privacy, numerous attempts have been made to introduce a systematization of the field (Bélanger & Crossler, 2011; Martin & Murphy, 2017). For the subsequent review of current approaches to privacy in communication and media research and to outline how the political dimension is implemented in these frameworks, we differentiate between approaches that either focus on privacy as individual boundary management or address the structural preconditions of privacy. This is related to Smith, Dinev, and Xu's (2011) value- vs. cognate-based approaches to privacy. Cognate-based concepts largely connect to psychological approaches and examine privacy primarily in relation to individuals' minds, perceptions, and cognition. The value-based approach encompasses an understanding of privacy as either a human right that is integral to society's moral value system or an economic commodity that is subject to potential exchange processes (Smith et al., 2011, p. 992). The individual–structure distinction strengthens what we believe is relevant to fostering political perspectives on privacy—namely, the interlinking of these two poles within a framework addressing the politics of privacy as a combination of agency and (limiting as well as enhancing) privacy (infra)structures (for a similar argument, see Baruh & Popescu, 2017).

2.1. Privacy as Individual Boundary Management

Studies examining privacy at the level of media users largely investigate the management of its boundaries with the intent to achieve a balance between the accessibility and withdrawal of their personal information or private life (Baruh, Secinti, & Cemalcilar, 2017). Conceptually, these approaches recur in Westin's privacy definition as an individual's control over what others know about him or her (Westin, 1967/2018). The regulation of access to the self (Margulis, 2011) thus remains primarily with individual subjects. As outlined by Regan (1995), Steeves (2009), and Sevignani (2016), this liberal understanding of privacy as an individual's personal right to balance or even defend against the interests of the society neglects the social dimension of privacy and its embeddedness in social relationships. The community functions of privacy are considered only implicitly. Although Steeves (2009, p. 194) has argued convincingly that Westin's conceptualization of privacy goes beyond the mere balancing of individual and societal needs, he has remained comparatively less outspoken in his work in regard to these arguments. Westin's understanding of privacy as the denial of access laid the foundation for Altman's (1975) view of how it is enacted in everyday life as a process of boundary control in which openness and closeness are optimized in the dialectical tension between them. Following Altman, privacy covers a broad spectrum ranging from social isolation (too much privacy) to a state of intrusion, whereby individuals have insufficient privacy. Altman's (1975) sociopsychological understanding of privacy thus allows us to capture the social embeddedness of privacy as interactions in which individuals engage "to negotiate the personal boundaries in their relationships" (Regan, 2015, p. 57). Arguing from an empirical perspective, Altman explicitly demanded that privacy be examined at the individual and group levels, and he put forward the notion of privacy as an

inherently social process (Margulis, 2003, p. 419). This conceptualization of privacy with a focus on an individual's opening and closing of boundaries between him or herself and others has, for instance, led to the development of Petronio's (1991) rule-based communication and Privacy Management Theory. According to the theory, privacy involves coordination with others. The Privacy Management Theory outlines five core principles that set the rules for managing one's privacy: (a) ownership of private information, (b) control through privacy rules, (c) coownership of shared information, (d) mutually agreed-upon privacy rules, and (e) consequences of boundary turbulence (Child & Petronio, 2011).

The examination of privacy as individual boundary management has influenced numerous empirical studies investigating privacy in interpersonal and computer-mediated communication environments. Researchers has also put forward the analysis of the conditions and factors influencing individuals' information-disclosing behaviors (Debatin, Lovejoy, Horn, & Hughes, 2009; Utz & Krämer, 2009). In particular, the so-called privacy paradox, which outlines the observed discrepancy between users' privacy attitudes and behaviors, has resulted in an extensive line of research (Dienlin & Trepte, 2015; Kokolakis, 2017).

Studying privacy from an individual boundary management perspective has also led to valuable insights into how media users manage their information sharing and the types of strategies, resources, and factors that impact their behaviors and attitudes. Despite Altman's (1975) conceptualization of privacy as socially constructed and embedded in social interactions, the consideration of how structural dimensions—for example, political or cultural contexts—impact these processes and how individuals' behaviors feed back into the structural conditions of interaction in (digital) media remain understudied. When the horizontal level of privacy—for example, the information exchange that takes place between media users—is analyzed, the vertical level—for example, individuals' attempts to protect their privacy against the intrusions of providers and institutions—tends to be overlooked. Masur (2019), for instance, pointed to the technical embeddedness of structural privacy, which remains "hidden behind the overt interfaces of the media in use" (p. 139). Privacy structures—users' (legal) rights and the politics of (private) companies' data collection practices and technologies—are largely considered (stable) contexts within which users negotiate their privacy. While the political dimension of privacy remains less emphasized in this stream of research, the notion of privacy as a collective (coownership of information) phenomenon, which is negotiated between individuals or groups, allows researchers to address its social relatedness.

2.2. The Structural Dimension of Privacy

According to Westin (2018), one can conceptualize privacy as a conflict between personal interests on the one hand and social interests on the other. Chmielewski (1991) expressed a similar viewpoint regarding anthropological investigations, explicating that privacy always arises when a society, and thus the public sphere, is formed: "In this sense privacy is a product or byproduct of the existence of society, especially of all those social institutions that control men's actions" (p. 268). In Western cultures, privacy is seen as an important prerequisite for an individual's autonomy and as a basic democratic value (Westin, 2003). In keeping with legal approaches to privacy, individuals lack the autonomy to exercise absolute control over their personal information; this is why privacy is viewed as a societal and political issue. From this viewpoint, individuals are not able to protect their privacy by themselves, nor are they fully responsible for doing so (Solove, 2002).

Some studies expand the focus on the legal-structural dimension of societal privacy regulation by integrating the individual level with regulatory approaches. The aim of these studies is to investigate the relationship between individuals' privacy attitudes and behaviors and the respective privacy governance system (for an overview, see Dogruel & Joeckel, 2019). The findings show how (national) cultural orientation shapes privacy orientation and regulation and vice versa (Bennett & Raab, 2018; Cockcroft & Rekker, 2016). In this regard, the societal regulation of privacy is expected to represent citizens' attitudes toward (informational) privacy—for example, their level of control over how their personal data are collected, processed, and used.

Beyond the legal approaches, the structural dimension of privacy covers the economic perspective. This views privacy as being subject to economic exchange processes that involve a negotiation between cost and benefit tradeoffs (Brandimarte & Acquisti, 2012). In this regard, users' information is considered to be business assets that can be traded—that is, exchanged for the targeted advertising or customization of products, messages, and prices (Acquisti, Taylor, & Wagman, 2015). Datafication—the transformation of social actions into quantifiable and trackable data (van Dijck, 2014)—has opened the path to large-scale economic and political surveillance practices and privacy invasion. Arguing from an economic perspective, the structural dimension of privacy has been explicated in most detail in the literature that adopts a critical perspective. This research stream addresses the commodification of privacy through the business models of online platforms (Sevignani, 2013). These companies largely rely on business models to exploit user data and transform online activities and private information into commodities. According to some scholars, the exploitation of privacy is connected to the emergence of a (new) platform capitalist model, which has given rise to data and surveillance capitalism (Lyon, 2019; West, 2019; Zuboff, 2015). The massive and systematic collection, processing, and use of Internet users' personal data enable the (asymmetrical) redistribution of power to platform providers who have access to and

capabilities for user data commodification (West, 2019). As highlighted in the introductory section, users are thus challenged to realize their desires for privacy become aware of the ability to create social interaction without opting out of capitalist platform services.

Studying privacy from a regulatory and economic perspective provides crucial insights into its structural preconditions. Researchers within this field focus on the emergence and change of collective institutional measures—that is, privacy governance—and the implications of such changes for privacy structures and privacy jurisdiction. Research also emphasizes the extent to which powerful actors, such as private corporations, and technology itself impact how privacy is enabled or limited within society. However, these approaches largely limit their analyses to the structural 'results'—namely, the emerging institutions, laws, unequal power distribution, or actual surveillance practices—while the analysis of the interrelations with users or citizens remains underdeveloped. This leaves considerable room for investigating how actors' agency—that is, users' doing of privacy—feeds back into the emergence and potential change of regulatory and economic power structures and thus has an overall effect on the process of politics.

3. Where Are the Politics?

Previous communication and media privacy research has been rather cautious in linking individual and structural dimensions of privacy. Legal scholars (Chesney & Citron, 2019; Cohen, 2013), for instance, discuss the constructed nature of the political self in relation to political, economic, and cultural environments. In their view, addressing privacy requires a discussion regarding the degree of political freedom or agency that is afforded by political systems or cultures. With an emphasis on technology, science and technology studies put forward similar views (Steijn & Vedder, 2015). During the last years, we see communication and media scholars addressing similar relations. However, although it is agreed that privacy *is* potentially political, it is difficult to grasp where it begins and ends. A brief examination of contemporary conceptual struggles over the definition of political communication illustrates that there are no straightforward answers: "Large-scale changes in the political economy of the world have altered international and domestic politics and thereby the grounds for political communication scholarship" (Moy, Bimber, Rojecki, Xenos, & Iyengar, 2012, p. 247). The media system has become blurred as platforms have gained a political role (Gillespie, 2010), and the distribution of news has shifted with the use of individual data (Bodó, Helberger, Eskens, & Möller, 2019). That is, former stable relationships between political power and communication are in transition, and new, politically relevant infrastructure is emerging (Bennett & Pfetsch, 2018). Similar arguments hold true for privacy, particularly when considering the relevance of the public and hidden governance of private communication infras-

tructure that bypass national media regulation or democratic control. But not everything that is related to the transformation of societies is necessarily political; there rather seems to have been a shift in what the realm of the political embraces.

What, then, is a useful definition of the political? Political theorists distinguish between two concepts of the political. It is denoted as "public debates about the right course in handling a collective problem…or the ability to make collectively binding decisions" (Zürn, 2015, p. 167). In other words, the political can be exercised via a joint communicative struggle over decision-making or through practices of power implementation. Communication and media scientists have been concerned primarily with the former, maintaining that calling the latter—that is, institutionalized politics—into question plays a considerable role in public debate. The distinction is helpful with regard to describing traditions of political thinking but hardly covers all contemporary modes of appearance—for instance, those related to privacy. Individual strategies, such as obfuscation (Brunton & Nissenbaum, 2016), may have a political character but are of collective relevance only if realized on a mass scale and in the long run.

Barry (2002) offered a helpful, broad, and rather functional, in contrast to procedural, distinction that was developed from an economic view. His discussion includes the role that technology plays in the transformation of power–communication relations. Barry's (2002) distinction aims to counteract approaches that locate the political "everywhere" (p. 269) and refers to 'the political' and 'politics' as two distinct realms. The political is a contested repertoire of options regarding how to approach a given societal problem; it is the realm of disagreement. An "action is political…to the extent it opens up the possibility for disagreement" (Barry, 2002, p. 270). Politics, in contrast, denotes practices that realize or limit these alternatives. Politics refers to "a set of technical practices, forms of knowledge and institutions," which are themselves the result of conflicts and agreements, whereas the political is "an index of the space of disagreement" (Barry, 2002, p. 270). While the political opens spaces for discussion and debate, politics institutionalizes single options—that is, by maintaining party discipline during parliamentary votes or by preparing a legislation process with regard to procedural affordances.

Barry's distinction between the political as a space of disagreement and politics as a set of reproductive or disruptive technological practices was originally designed to embrace the interrelationship between politics and political communication with a view to achieving an increasingly politicized economy in contrast to limiting political diversity. When his article was published, data politics and governance were on the verge of emerging but were hardly a general topic of academic debate. Contemporary social sciences offer a different view by discussing technology as neatly interwoven with both politics and the political. Privacy research shows that the

political can have a very technical and practical character. Hacking (Kubitschko, 2017) or avoiding insecure messengers (Kannengießer, 2020) can be a practical measure in the sense of political alternatives. Other (mass) practices, such as sharing data via cookies or the mass use of messengers, could be considered politics because they foster dominant economy-driven privacy regimes.

Barry's approach has two clear advantages when seeking to systematize approaches to the political implications of privacy. First, his perspective avoids references to political or media systems as a predefined (geographic) space, which is crucial when considering privacy as a practice that embraces activities beyond the national, legal, or technological contexts (Milan & Hintz, 2013). The political as the realm of contestation over options for approaching an issue exists in general but has no clear boundary, such as a national public sphere; it is considerably limited by politics. Barry underscored that as different groups, political power holders, entrepreneurs, or activists dispose of diverse instruments to channel the space of contestation, which ranges from political debate or censorship to products that are offered or used. As politics and the political are always related, spaces of contestation can be narrow or ample irrespective of political or media systems. He highlights that:

> What is commonly termed politics is not necessarily—or generally—political in its consequences. Politics can often be profoundly anti-political in its effects: suppressing potential spaces of contestation; placing limits on the possibilities for debate and confrontation. Indeed, one might say that one of the core functions of politics has been, and should be, to place limits on the political. (Barry, 2002, p. 270)

Second, Barry explicitly considered the political role of technology. According to him, technologies created "effects of placing actions and objects (provisionally) outside the realm of public contestation" (2002, p. 271). This is a key issue for privacy researchers, as technologies program the way in which users realize privacy on an everyday basis. Privacy as a political issue refers to a contesting field of solutions for how to exert control over the flow of information and communication. The politics of technologies can broaden this space, for instance, by providing alternative solutions and techno-educational activities (Kannengießer, 2020) or can limit it by downplaying their political impact (Gillespie, 2010).

4. Sorting Perspectives on the Political Implications of Privacy

As a political concept, privacy emerges when it is considered beyond the individual concerns of balancing, agency, data security, and public participation (Cohen, 2013). Although communication and media privacy researchers have investigated many related aspects, a systematic overview is missing. By developing a roadmap to sort research questions that address the political dimensions of privacy, we benefit from the previously outlined thorough debate regarding contemporary privacy research and the distinctions between approaches to the political, as offered by Barry. In keeping with this, we conclude that political perspectives on privacy *relate* individuals and structures. Privacy researchers address political aspects when considering the consequences of individual actions vis-à-vis structured surroundings. Similarly, the investigation of rules, institutions or technology has a political character when the consequences for agency are taken into account. This is why we speak of agency instead of individual perspectives on privacy. Terms such as 'civic action' would not be suitable in this context, as negotiations on what constitutes public and private boundaries occur inside, outside, and beyond political systems (we borrowed this distinction from Milan & Hintz, 2013). The second dimension adheres to Barry (2002) by pointing to the two equally related realms of politics and the political. We consider the analysis of any action or practice political in cases in which it relates to the realm of political options or alternatives, whether it is confirming or limiting options. The political realm of privacy entails the various contested privacy options, which can be offered in discourse or as a technical alternative.

Both axes form a four-field matrix that allows to map scholarly perspectives on the political implications of privacy (see Figure 1). The objective of this matrix is to guide the organization of existing and emerging approaches to the political implications of privacy. We suggest distinguishing privacy as (a) emerging rules or (b) discourses, as (c) programmed, or as (d) media practices. While scholarly work must not clearly be subsumed under a single label, doing so allows us to identify more (or less) pronounced implications of the political dimension of privacy, which can even vary across a scholar's work. For instance, Regan (1995, 2016), a researcher who is well known for her scholarly work on privacy as discourse, has regularly highlighted normative privacy threats. In her later work, she explored privacy threats vis-à-vis digital youth (Steeves & Regan, 2014), focusing on privacy as media practices.

First, the perspectives on privacy as emerging rules highlight that particular privacy rules apply in specific contexts. This view critically addresses access—and control understandings of privacy, focusing on individual notice and choice decisions regarding sharing or granting access to information (Martin, 2016, p. 552). Instead, privacy as emerging rules approaches argue that "individuals give access to information…with an understanding of the privacy rules that govern that context" (Martin, 2016, p. 553)—that is, depending on the given social relations. Nissenbaum (2010, 2019) coined the term 'contextual integrity' to describe this societal quality of privacy. In contrast, arguing from an organizational studies perspective, researchers put forward the idea of privacy as a 'social contract' (Culnan & Bies, 2003; Martin, 2016). Both perspectives are based on the premise that privacy
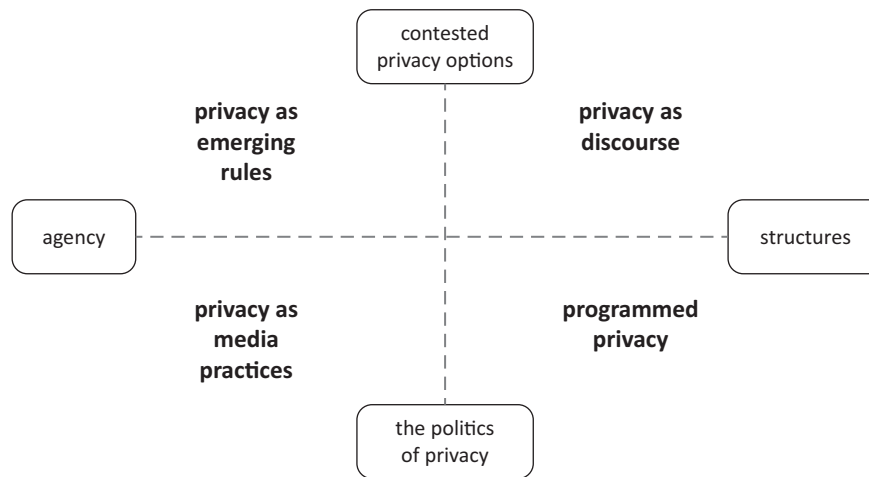
Figure 1. Four perspectives on the political implications of privacy.

is not about data protection but about the appropriate flow of information. Focusing on the outcomes—that is, the rules and norms of social privacy contracts—rather than on the processes, this view plays a role in business perspectives. Researchers are interested in understanding the diverging privacy expectations of groups of individuals. Consumers, for instance, would react differently to sharing retail data than they would to sharing financial data (Martin, 2016, p. 564), which would impact the design of product portfolios.

From a political viewpoint, this perspective challenges normative accounts of privacy that deals with ready-made measures for data security and involvement. Nissenbaum's (2010, 2019) key argument is that privacy technology and everyday practices are in constant transition, as are the emergent privacy relations and norms. Compliance with these norms is a precondition for responsive and appropriate politics. Expecting that voting behavior would remain private information, platforms such as the NationBuilder transgress these boundaries (McKelvey, 2019). The political character of privacy thus emerges when comparing privacy norms implemented in legal or economic contexts to their emerging appropriateness as a benchmark (Nissenbaum, 2019, p. 234), taking into account that this appropriateness is a societal, privacy practice-based compromise. This non-media-centric and practice-oriented perspective raises critical questions regarding the existential threats to privacy via datafication and digitization. In this regard, Nissenbaum (2019, p. 238) states the following: "A prevailing political economy that is lax—or one might say, friendly—in its regulation of the information industries has allowed the consolidation of data into massive centers, ultimately funneled into the hands of relatively few proprietors."

Second, in contrast to the perspectives on privacy as emerging rules, privacy discourse perspectives depart from the assumption that the way in which cultural, political, or technological agents legitimize privacy matters for its societal, institutional, or infrastructural implementation. This relationship represents a crucial dimension of Internet governance in general (Epstein, Katzenbach, & Musiani, 2016). The privacy discourse perspective applies to scholarly work that itself strives to broaden the repertoire of privacy conceptions (Brunton & Nissenbaum, 2016; Regan, 2002). Researchers applying this perspective consider Nissenbaum's contextual integrity from the other side; that is, they strive to understand what is common and shared. Greene and Shilton (2017) provided a best-case study to illustrate this basic assumption as they crossed the boundaries of a single-discourse analysis. They focused on the relationship between platform privacy governance and software developers' (absent) autonomy to define privacy. Analyzing both debates on platform and among developer, the authors demonstrated how the latter subordinate their definitory autonomy.

Greene and Shilton's (2017) study on platform politics can equally be considered a study applying the programmed privacy perspective. Subordinate to their discourse analysis, they demonstrated how software developers "in return for access to a centralized portal that provides access to customers and lowers distribution costs…must accept more centralized forms of control" (Greene & Shilton, 2017, p. 1643). The programmed privacy view is mainly concerned with the relationship between infrastructure and privacy politics. Researchers ask which practices limit or confirm political privacy solutions and how. For instance, Gürses, Kundnani, and van Hoboken (2016) and Baruh and Popescu (2017) investigated how technologies limit or increase the privacy options available to marginalized groups. The transparency of technology programs—that is, their inscribed rules—are a normative claim often raised in this approach (see, e.g., Diaz & Gürses, 2012).

Similar views are addressed in more critical contributions to privacy and technology. Taylor, Floridi, and van der Sloot (2017a) offered insights into the role that technology plays in group-defining processes. In an age of big data, individuals and their social contexts, as put

forward in contextual integration theory, are not of primary interest, but their joint uses of media technologies allow for the analysis of types and clusters. Taylor, Floridi, and van der Sloot (2017b, p. 5) claimed that "technologies actually determine groups, through their clustering and typification," with predictability rising with group size (Sarigol, Garcia, & Schweitzer, 2014). Similar arguments can be found in the work of scholars who adopt a critical political economics perspective, such as Fuchs (2011, 2013) or Sevignani (2013). In their work, platforms are analyzed against the background of their capitalist intentions, treating users' privacy as a commodity. Focusing on how technology impacts structural privacy, Yeung (2017) explicated how technological architecture and website design were found to exert control over how privacy is approached in society.

Finally, we describe the perspectives on privacy as media practices, which overlap to some extent with the programmed privacy view, as the former focuses on routinized action that confirms or limits contested privacy alternatives. However, it differs from it with respect to its focus on agency instead of infrastructures. Scholarly work emphasizing the political implications of privacy adheres to the media practice approach put forward by Couldry (2004) and others (Kaun, 2015; Mattoni, 2012; Mattoni & Treré, 2014). This view transcends the focus on technology as guiding infrastructure and emphasizes that social order is enacted through repetition and routine on the one hand or disruptive action on the other. Kubitschko (2017) and Kannengießer and Kubitschko (2017) introduced a differentiation between media practices according to their political qualities. Acting *with* media means having it at one's disposal as they are offered—that is, using Google as a search engine or providing data when shopping online. In contrast, acting *on* media denotes practices that are aimed at shaping media infrastructure—that is, hacking (Kubitschko, 2017) or obfuscation strategies (Brunton & Nissenbaum, 2016). Acting on media also embraces the discursive level of action—that is, contributing to the discourses on surveillance technologies (Möller & Mollen, 2017). Thus, acting on media covers a whole repertoire of actions ranging from direct technical interventions to advocacy and educational activities. That is, privacy media practices are structured but must not necessarily be conscious acts.

This approach is particularly suited to embracing the ambiguities of digital citizenship—that is, privacy as a constant endeavor to embrace both participation and the pitfalls of data security. Hintz et al. (2019, p. 3) stated convincingly that:

> Datafication may generate new possibilities for citizen action, but it may also create and reinforce inequalities, differences and divisions…, the processing of data has become a cornerstone of contemporary forms of governance as it enables both corporate and state actors to profile, sort and categorize populations.

This perspective is not limited to the consideration of civic actors but favors them in the cases in which the political consequences of acting with media are of interest. Nonetheless, this view is applicable to economic or political power holders' media practices. For instance, without explicit reference to the media practice approach, Susser et al. (2019) pointed out that new power arrangements go far deeper than threatening the interests of individuals; they also affect collective values (e.g., through large-scale political and economic manipulation) and thus need to be considered a political issue as well.

5. Discussion and Outlook

Scholarly work on the management of information boundaries shows that privacy is an ambiguous concept. Individual strategies are inseparably associated with group relationships or structural conditions. In fact, according to Stahl (2016), "what privacy protects us from is not interference but domination" (p. 34). Interference with data is just as normal as data sharing, with all of its related risks and benefits. Privacy is not only about information security but is also about finding a balance between being part of communities, groups, and societies, as well as observation/control/rules while maintaining individual or group agency. At the same time, privacy is a value in itself. A lack of boundary reflection and management complicates social coexistence. Communication and media scholars increasingly harness the participation–data security ambiguity and the normativity of privacy to address ongoing societal change. Herein, privacy is a useful tool for approaching the contemporary challenges of balancing participation or agency and the risks related to sharing individual or organizational information.

Against this background, this contribution maps the various perspectives on privacy politics that emerge at the crossroads between communication and media research and the work that is carried out in other disciplines. We believe that scholarly communication and media views on the political dimensions of privacy can benefit from a clearer outline of which political dimension of privacy their work refers to. Based on discourses on the societal and relational nature of privacy, as well as the distinction between politics and the political, we outlined four perspectives on the political implications of privacy, privacy as emerging rules and discourse, programmed privacy, and privacy as media practices. With this contribution, we have provided a heuristic that allows media scholars to position themselves among the myriad approaches to the politics of privacy, ranging from the individual level of personal privacy to the societal struggle for privacy norms and regulations, and to be clear on what they have in mind when discussing the political implications of privacy.

References

Acquisti, A., Taylor, C. R., & Wagman, L. (2015). The economics of privacy. *Journal of Economic*, *52*(2). http://dx.doi.org/10.2139/ssrn.2580411

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

Barry, A. (2002). The anti-political economy. *Economy and Society*, *31*(2), 268–284. https://doi.org/10.1080/03085140220123162

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

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

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. https://doi.org/10.1111/ips.12048

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in informationsystems. *MIS Quarterly*, *35*(4), 1017–1041.

Bellanova, R. (2017). Digital, politics, and algorithms. *European Journal of Social Theory*, *20*(3), 329–347. https://doi.org/10.1177/1368431016679167

Bennett, C. J., & Raab, C. D. (2018). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance*, *1*(6), 142. https://doi.org/10.1111/rego.12222

Bennett, W. L., & Pfetsch, B. (2018). Rethinking political communication in a time of disrupted public spheres. *Journal of Communication*, *68*(2), 243–253. https://doi.org/10.1093/joc/jqx017

Bodó, B., Helberger, N., Eskens, S., & Möller, J. (2019). Interested in diversity. *Digital Journalism*, *7*(2), 206–229. https://doi.org/10.1080/21670811.2018.1521292

Brandimarte, L., & Acquisti, A. (2012). The economics of privacy. In M. Peitz & J. Waldfogel (Eds.), *Oxford handbooks in economics: The Oxford handbook of the digital economy* (pp. 547–671). Oxford: Oxford University Press.

Bräunlich, K., Dienlin, T., Eichenhofer, J., Helm, P., Trepte, S., Grimm, R., . . . Gusy, C. (2020). Linking loose ends: An interdisciplinary privacy and communication model. *New Media & Society*. https://doi.org/10.1177/1461444820905045547

Brunton, F., & Nissenbaum, H. (2016). *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: MIT Press.

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*, 1753–1820. https://doi.org/10.15779/Z38RV0D15J

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the Internet. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 21–40). New York, NY: Peter Lang.

Chmielewski, P. (1991). The public and the private in primitive societies. *International Political Review*, *12*(4), 267–280. https://doi.org/10.1177/019251219101200402

Cockcroft, S., & Rekker, S. (2016). The relationship between culture and information privacy policy. *Electron Markets*, *26*(1), 55–72. https://doi.org/10.1007/s12525-015-0195-9

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, *126*, 1904–1933.

Couldry, N. (2004). Theorising media as practice. *Social Semiotics*, *14*(2), 115–132. https://doi.org/10.1080/1035033042000238295

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323–342. https://doi.org/10.1111/1540-4560.00067

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society*, *22*(7), 873–881. https://doi.org/10.1080/1369118X.2019.1606268

Diaz, C., & Gürses, S. (2012). *Understanding the landscape of privacy technologies*. Leuven: KU Leuven. Retrieved from https://www.esat.kuleuven.be/cosic/publications/article-2215.pdf

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dogruel, L., & Joeckel, S. (2019). Risk perception and privacy regulation preferences from a cross-cultural perspective: A qualitative study among German and U.S. smartphone users. *International Journal of Communication*, *13*, 1764–1783.

Epstein, D., Katzenbach, C., & Musiani, F. (2016). Doing internet governance: Practices, controversies, infrastructures, and institutions. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.435

Fuchs, C. (2011). The political economy of privacy on Facebook. *Television & New Media*, *13*(2), 139–159. https://doi.org/10.1177/1527476411415699

Fuchs, C. (2013). Societal and ideological impacts of deep packet inspection internet surveillance. *Information, Communication & Society*, *16*(8), 1328–1359. https://doi.org/10.1080/1369118X.2013.770544

Gillespie, T. (2010). The politics of 'platforms.' *New Media & Society*, *12*(3), 347–364. https://doi.org/10.1177/1461444809342738

Greene, D., & Shilton, K. (2017). Platform privacies: Governance, collaboration, and the different meanings of 'privacy' in iOS and Android development. *New Media & Society*, *126*(3), 1640–1657. https://doi.org/10.1177/1461444817702397

Gürses, S., Kundnani, A., & van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society*, *38*(4), 576–590. https://doi.org/10.1177/0163443716643006

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). *Digital citizenship in a datafied society*. Medford, MA: Polity Press.

Kannengießer, S. (2020). Fair media technologies: Innovative media devices for social change and the good life. *The Journal of Media Innovations*, *6*(1), 38–49. https://doi.org/10.5617/jomi.7832

Kannengießer, S., & Kubitschko, S. (2017). Acting on media: Influencing, shapingand and (re)configuring the fabric of everyday life. *Media and Communication*, *5*(3), 1–4. https://doi.org/10.17645/mac.v5i3.1165

Katzenbach, C., & Bächle, T. C. (2019). Defining concepts of the digital society. *Internet Policy Review*, *8*(4), 1–6. https://doi.org/10.14763/2019.4.1430

Kaun, A. (2015). "This space belongs to us!": Protest spaces in times of accelerating capitalism. In L. Dencik & O. Leistert (Eds.), *Critical approaches to social media protest: Contentions and debates* (pp. 91–110). London: Rowman & Littlefield Publishers.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kubitschko, S. (2017). Acting on media technologies and infrastructures: Expanding the media as practice approach. *Media, Culture & Society*, *21*(3). https://doi.org/10.1177/0163443717706068

Lokot, T. (2018). Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society*, *16*(3), 332–346. https://doi.org/10.24908/ss.v16i3.6967

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics* (pp. 64–77). Abingdon and New York, NY: Routledge. https://doi.org/10.4324/9781315167305-4

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, *59*(2), 411–429. https://doi.org/10.1111/1540-4560.00071

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). Berlin and Heidelberg: Springer.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, *137*(3), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Masur, P. K. (2019). *Situational privacy and self-disclosure*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78884-5

Mattoni, A. (2012). *Media practices and protest politics: How precarious workers mobilise*. Aldershot: Ashgate Publishing.

Mattoni, A., & Treré, E. (2014). Media practices, mediation processes, and mediatization in the study of social movements. *Communication Theory*, *24*(3), 252–271. https://doi.org/10.1111/comt.12038

Matzner, T., & Ochs, C. (2019). Privacy. *Internet Policy Review*, *8*(4), 1–14. https://doi.org/10.14763/2019.4.1427

McKelvey, F. (2019). Cranks, clickbait and cons: On the acceptable use of political engagement platforms. *Internet Policy Review*, *8*(4), 1–27. https://doi.org/10.14763/2019.4.1439

Milan, S., & Hintz, A. (2013). Networked collective action and the institutionalized policy debate: Bringing cyberactivism to the policy arena? *Policy & Internet*, *5*(1), 7–26. https://doi.org/10.1002/poi3.20

Möller, J., & Mollen, A. (2017). "Please stay frustrated!" The politicisation of media technologies in the German NSA debate. In R. Kunelius, H. Heikkilä, A. Russell, & D. Yagodin (Eds.), *Journalism and the NSA revelations* (pp 113–127). Oxford: Reuters Institute for the Study of Journalism.

Moy, P., Bimber, B., Rojecki, A., Xenos, M. A., & Iyengar, S. (2012). Shifting contours in political communication research. *International Journal of Communication*, *6*, 247–254.

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

Nissenbaum, H. (2019). Contextual integrity up and contextual integrity up and down the data food chain. *Theoretical Inquiries in Law*, *20*(1), 221–256.

Petronio, S. (1991). Communication boundary manage-

ment: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, *1*(4), 311–335. https://doi.org/10.1111/j.1468-2885.1991.tb00023.x

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, NC: University of North Carolina Press. https://doi.org/10.5149/9780807864050_regan

Regan, P. M. (2002). Privacy as a common good in the digital world. *Information, Communication & Society*, *5*(3), 382–405. https://doi.org/10.1080/13691180210159328

Regan, P. M. (2015). Privacy and the common good: Revisited. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 50–70). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781107280557.004

Regan, P. M. (2016). Response to privacy as a public good. *Duke Law Journal Online*, *65*(51), 51–65.

Rose, A., Littleboy, S., Bruggeman, J., & Rao, A. (2018). WhatsApp doc: Legal and practical perspectives of using mobile messaging. *Digital Health*. Retrieved from https://www.digitalhealth.net/2018/02/whatsapp-doc-legal-and-practical-perspectives-of-using-mobile-messaging

Sarigol, E., Garcia, D., & Schweitzer, F. (2014). Online privacy as a collective phenomenon. In *COSN '14: Proceedings of the second ACM conference on online social networks*. Retrieved from https://arxiv.org/abs/1409.6197

Sevignani, S. (2013). The commodification of privacy on the Internet. *Journal of Social Issues*, *40*(6), 733–739. https://doi.org/10.1093/scipol/sct082

Sevignani, S. (2016). *Privacy and capitalism in the age of social media*. London and New York, NY: Routledge and Taylor & Francis Group.

Singer, N., & Sang-Hun, C. (2020, March 23). As coronavirus surveillance escalates, personal privacy plummets. *The New York Times*. Retrieve from https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

Smith, H. J., & Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1156. https://doi.org/10.2307/3481326

Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology*, *18*(1), 33–39. https://doi.org/10.1007/s10676-016-9392-2

Steeves, V. M. (2009). Reclaiming the social value of privacy. In I. Kerr, C. Lucock, & V. M. Steeves (Eds.),

Lessons from the identity trail: Anonymity, privacy and identity in a networked society (pp. 191–208). Oxford and New York, NY: Oxford University Press

Steeves, V. M., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313. https://doi.org/10.1108/JICES-01-2014-0004

Steijn, W. M. P., & Vedder, A. (2015). Privacy under construction: A developmental perspective on privacy perception. *Science, Technology, & Human Values*, *40*(4), 615–637. https://doi.org/10.1177/0162243915571167

Susser, D., Roessler, B., & Nissenbaum, H. F. (2019). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review*. http://dx.doi.org/10.2139/ssrn.3306006

Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017a). *Group privacy: New challenges of data technologies*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8

Taylor, L., Floridi, L., & van der Sloot, B. (2017b). Introduction. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group privacy: New challenges of data technologies* (pp. 1–11). Cham: Springer International Publishing.

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2).

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

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

Westin, A. F. (2018). *Privacy and freedom*. New York, NY: IG Publishing. (Original work published 1967)

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society, 20*(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zürn, M. (2015). Opening up Europe: Next steps in politicisation research. *West European Politics*, *39*(1), 164–182. https://doi.org/10.1080/01402382.2015.1081513

About the Authors

Johanna E. Möller is a Post-Doc Researcher at the Department of Communication at Johannes Gutenberg University Mainz, Germany. Her scholarly work is located at the intersection of media sociology, political communication and media economics. She works on the datafication of societies, political and economic agency and communication and media theory. https://orcid.org/0000-0003-4377-2206

Leyla Dogruel is Assistant Professor at the Department of Communication at Johannes Gutenberg University Mainz, Germany. Her areas of research focus on privacy in mobile media, decision making in digital media, media innovation and media change. https://orcid.org/0000-0003-2701-3402