Media and Communication

Open Access Journal | ISSN: 2183-2439

Volume 8, Issue 2 (2020)

# The Politics of Privacy: Communication and Media Perspectives in Privacy Research

Editors

Johanna E. Möller, Jakub Nowak, Sigrid Kannengießer
and Judith E. Möller

COGITATIO

Media and Communication, 2020, Volume 8, Issue 2
The Politics of Privacy: Communication and Media Perspectives in Privacy Research

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070-129 Lisbon
Portugal

*Academic Editors*
Johanna E. Möller (Johannes Gutenberg University Mainz, Germany)
Jakub Nowak (Maria Curie-Sklodowska University, Poland)
Sigrid Kannengießer (University of Bremen, Germany)
Judith E. Möller (University of Amsterdam, The Netherlands)

Available online at: www.cogitatiopress.com/mediaandcommunication

# Table of Contents

COGITATIO

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 2, Pages 232–236
DOI: 10.17645/mac.v8i2.3373

Editorial

# The Politics of Privacy—A Useful Tautology

Johanna E. Möller [1,*], Jakub Nowak [2], Sigrid Kannengießer [3] and Judith E. Möller [4]

[1] Department of Communication, Johannes Gutenberg University Mainz, 55128 Mainz, Germany;
E-Mail: johanna.moeller@uni-mainz.de
[2] Institute of Social Communication and Media Studies, Maria Curie-Skłodowska University, 20-031 Lublin, Poland;
E-Mail: jakub.nowak@poczta.umcs.lublin.pl
[3] Center for Media, Communication and Information Research, University of Bremen, 28359 Bremen, Germany;
E-Mail: sigrid.kannengiesser@uni-bremen.de
[4] Amsterdam School of Communication Research, University of Amsterdam, 1018XE Amsterdam, The Netherlands;
E-Mail: j.e.moller1@uva.nl

* Corresponding author

Submitted: 17 June 2020 | Published: 23 June 2020

**Abstract**

While communication and media studies tend to define privacy with reference to data security, current processes of datafication and commodification substantially transform ways of how people act in increasingly dense communicative networks. This begs for advancing research on the flow of individual and organizational information considering its relational, contextual and, in consequence, political dimensions. Privacy, understood as the control over the flow of individual or group information in relation to communicative actions of others, frames the articles assembled in this thematic issue. These contributions focus on theoretical challenges of contemporary communication and media privacy research as well as on structural privacy conditions and people's mundane communicative practices underlining inherent political aspect. They highlight how particular acts of doing privacy are grounded in citizen agency realized in datafied environments. Overall, this collection of articles unfolds the concept of 'Politics of Privacy' in diverse ways, contributing to an emerging body of communication and media research.

**Keywords**

agency; datafication; data security; media practices; politics; privacy

**Issue**

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

In datafied societies privacy practices are under pressure. Defining datafication as a meta process which "render[s] into data many aspects of the world that have never been quantified before" (Cukier & Mayer-Schoenberger, 2013, p. 29), and as a "means to *access*, *understand* and *monitor* people's behavior" (van Dijck, 2014, p. 189), we perceive changes and challenges with respect to the politics of privacy—changes and challenges which are intertwined. Private data is collected, archived and used for analytical and strategic means in often opaque ways. From a critical point of view, datafied communication is based on a political-economic formation that "relieves top-level actors (corporate, institutional and governmental) from the obligation to respond" (Dean, 2005, p. 53), while fighting for dominance over access to useful data. At the level of agents or citizens this implies practical challenges, such as finding new ways to deal with public visibility and participation (Birchall, 2016) or developing the ability to reflect on data flows (Kannengießer, 2019).

Considering these changes and challenges, it is worth highlighting that privacy is distinct from data security. Both embrace practices aimed at data protection, but data security denotes the safeguarding of private information from unwanted interference by agents, technologies or legislation. This way, data or information would remain secret unless revealed on purpose by data owners and agents in control of these closed doors. The concept of privacy, in contrast, acknowledges that datafied communication is necessarily interrelated and interconnected (boyd, 2012). Privacy refers to the demarcation of communication flow boundaries. Privacy is embedded in society and neatly interwoven with the everyday communicative action of social and political actors. While data security requires communication and media literacy or adequate data policies, privacy has more profound political implications since, for instance, communication infrastructures determine privacy conditions and, vice versa, so that mundane communicative action can become a form of politics by consumption (Stolle, Hooghe, & Micheletti, 2005).

As such we suggest understanding privacy as the control over the flow of individual or organizational information in relation to the action of others. These relations are shaped by the media environment, information infrastructure, and societal or cultural rules in which they are formed. Understanding privacy as ‘control over’ is an ideal. Absolute control is not possible, which means in practice that privacy is understood as the *attempt* to exercise control over the flow of individual or organizational information. To pursue privacy is to seek to realize this control in relation to others—as privacy is relational, collective, context-related and, as a result, constantly evolving (Möller & Nowak, 2018). Speaking of the politics of privacy, thus, is a tautology that, yet, embraces the attempts assembled in this thematic issue to explore these political dimensions.

Communication and media studies, so far, tend to define privacy in close relation to data security. The private is conceptualized as the opposite to the public, for instance, a protected space where opinions are formed (Bentele & Nothhaft, 2010). This is equally true of more dynamic cultural studies approaches (Livingstone, 2015). Data security is also instructive for academic work in the realm of media psychology where scholars focus on privacy literacy and related strategies (Masur, 2018; Trepte, Scharkow, & Dienlin, 2020). Researchers in this field point to the paradoxical relation between knowledge about privacy risks and actual data protection practices. For a couple of years now, nevertheless, we have seen a new development. Communication and media researchers have started to re-engage with privacy as a *societal* concept (Matzner & Ochs, 2019; Möller & Nowak, 2018). Understanding privacy as embedded in communicative infrastructures broadens perspectives held by communication and media scholars. Recent studies show that privacy embraces manifold online and offline, public and hidden social practices during which actors create processes or entities that are closed to others.

The articles assembled in this thematic issue contribute to the reinvigorating communication and media privacy research and prepare the ground for further research on the often surprising and far-reaching political and societal implications of privacy. The contribution of media psychologist Philipp K. Masur (2020), for instance, illustrates this shift in perspective. Offering a holistic model of critical online privacy literacy, he critically addresses notions of privacy as freedom from intrusion. Academic and data artist Luke Munn (2020) queries the widely shared assumption that decentralized data collection is privacy friendly by nature and offers more control to individuals. Instead, edge computing apparently circumvents data protection and continues centralized data collection. Grażyna Stachyra (2020), to mention a final example, carefully carves out the political nature of contemporary radio practices. While radio has a history of and reputation for safeguarding individual data, in its current converged form, it may affect the privacies of unintended participants in radio shows around the globe.

Privacy is an interdisciplinary field of research by default. Historians (Igo, 2018), sociologists (Lyon, 2018) or information scientists (Nissenbaum, 2010), just to name some disciplines, have made substantial contributions to advancing understandings of its political nature. But what can communication and media scholars contribute to this? Communication and media researchers observe people’s mundane communicative action. They understand how deeply this action is interwoven with its structured surroundings. While datafication and commodification substantially transform political, economic and societal environments (Hintz, Dencik, & Wahl-Jorgensen, 2017; Lyon, 2018), researchers explore how individuals accompany and co-carry these processes through their interrelated communicative networks. Also, communication and media scientists benefit from “polymedia” perspectives (Madianou & Miller, 2012), whereby they embrace analyses of communicative action across media repertoires and non-mediated communication. This helps to avoid techno-centric perspectives that easily emerge in privacy research. Moreover, communication and media scholars stress critical reflection and agency, both incremental drivers for people’s conceptions of privacy. Means and perspectives in the field are designed to make it possible to grasp these conceptions’ contextual roots in culture or patterns of power. Privacy has become the very center of what it means to be a citizen nowadays, affecting how people act in private and in public, and how they socialize. Therefore, privacy has a deep political meaning that leads authors in articles assembled in this thematic issue to reflect on the theoretical quality of the ‘Politics of Privacy.’

Conceptualizing privacy and its political dimensions calls for theoretical work. Johanna E. Möller and Leyla Dogruel (2020) offer a theoretical framework to map further empirical work in the field. These authors closely review the field of media privacy research focusing on its political dimension and on this basis leverage Barry's (2002) differentiation between politics and the political. The concepts of the political and politics lead them to differentiate between individual and structural dimensions of privacy and develop a matrix through which political implications of media related privacy can be investigated. Within this matrix they distinguish between privacy as: 1) emerging rules; 2) discourses; 3) programmed privacy; and 4) media practices. Acknowledging these dimensions, media and communication scholars can position themselves in the complex research field of privacy while at the same time theorizing and analyzing the politics of privacy.

Another article in the issue that critically approaches the prevailing discursive constructions in contemporary debate on privacy and surveillance is Heikki Heikkilä's (2020) contribution. The author questions the dominant discursive dialectic opposition of surveillance and privacy ('moral coupling'), in which both phenomena are depicted as mutually oriented contradictions with opposing normative evaluations—surveillance being wrong and privacy being good. This simplistic discursive position, Heikkilä argues, does not respond to how privacy is approached and realized nowadays, as it overlooks the ambiguities of how people construct their online privacies and underlying definitions of both privacy and its intrusions. Therefore, more nuanced and context-related notions should be elaborated and pursued, also taking under consideration very personal experiences and life situations of individuals. Heikkilä proposes a framework for such empirical privacy studies that acknowledges these ambiguities, and, thus, has the potential to go beyond discursive moral coupling of privacy and surveillance.

In his theoretical contribution, Philipp K. Masur (2020) challenges the dominant paradigm of privacy protection by proposing a holistic model of critical online privacy literacy. Masur grounds his argument in critiquing the negative perspective of privacy, and presents a model of online privacy literacy that comprises privacy knowledge, privacy-related reflection abilities, privacy and data protection skills, and critical privacy literacy. This combination of knowledge, technical abilities, and the conscious recognition of sociopolitical relations shaping technological environments, the author argues, enables individuals not only to protect themselves more against privacy violations, but also may motivate them to critically challenge the dominant individualistic paradigm of privacy that necessitates the need for protection in the first place. As a result, this shift in perspective, as described in Masur's article, correlates to an increased motivation to participate in democratic processes that may affect how privacy is approached or realized also on the levels of discourse or politics.

Following these theoretical considerations, Luke Munn (2020) critically investigates the privacy implications of edge computing and showcases the importance of interdisciplinary approaches to the question of privacy. From a technical perspective, edge computing is often hailed as a way to guarantee privacy while still granting users all the convenience of personalized services. If the data is not transmitted to a central data processing service in the cloud but stays on the device, privacy risks should be minimized. Munn, however, finds that the affordances of edge computing sidestep established safeguards, because edge data, after privacy 'sterilization,' can still be stored in conventional data centers. This leads to new risks and requires new responses both on the regulatory and the citizen-led level.

Grażyna Stachyra (2020) offers another in-depth empirical study of privacy policies and practices in radio—a medium that has a history of and a reputation for being a privacy friendly medium. In contrast to this ideal, Stachyra's analysis shows how contemporary converged and transnational radio practices affect the privacies of unintended participants in their shows. In December 2012, Jacintha Saldanha, nurse at London's Royal King Edward VII Hospital committed suicide after two Australian radio presenters had made a prank phone call pretending to be Queen Elizabeth and Prince Charles showing concern about the state of Duchess Kate's health while expecting her first child. The case reveals three conditions which have implications for persons unintentionally involved: 1) digitization renders radio content archivable; 2) the division of radio related labor leads to a loss of journalistic responsibility and sensitivity with regard to private information; 3) legal frameworks continue to apply legacy radio privacy measures and do not correspond to these new working conditions.

The contribution by Yannic Meier, Johanna Schäwel and Nicole C. Krämer (2020) points out that although privacy is often regarded and measured as a general privacy concern, it is challenged in specific situations. A typical situation is when users are asked to provide data online. Data protection regulation such as the EU General Data Protection Regulation (GDPR) requires websites to display privacy policies and ask for active consent to minimize privacy risks. The authors question the extent to which this consent is meaningful, given that users often do not engage with the lengthy privacy policies, let alone process the information they obtain. Using a survey experiment they find that readers of shorter policies spend less time reading but learned more about the content through an indirect effect mediated by time spent per word. Shorter policies can thus be both more efficient and more effective.

Two more contributions complete these insights as they shed light on culturally specific discursive contexts of privacy. Łukasz Wojtkowski, Barbara Brodzińska-Mirowska and Aleksandra Seklecka (2020) take on a previous research gap by investigating privacy frames in the Polish media discourse. This debate meets all requirements for an intense and in-depth debate of privacy related issues in its manifold contextual, relational, cultural and political aspects. Poland looks back on a communist history with invasive surveillance practices, also Polish media debates are characterized by heavy polarization and the contemporary government favors privacy unfriendly policies. Against this background it is surprising that the authors find the Polish privacy debate seems to be still in its early stages. Across the Polish media landscape, outlets mainly address political challenges resulting from European data protection politics. Not uncommon are complaints about how the GDPR restricts election campaigning or governmental projects.

In her analysis, Tetyana Lokot (2020) contrasts Russian state officials' and digital rights advocates' privacy constructions as found in their public discourses. Based on an extant analysis of online documents provided by the state's telecom regulator "Roskomnadzor" and digital activists "Roskomsvoboda," Lokot shows that diverging conceptualizations of privacy are a key indicator for conflicts about how to approach the political. More than that, struggle for access to individual data is one of the arenas in which the fight for power and control in the Russian hybrid political system takes place. Lokot, not least, contributes a valuable methodological proposal. Her study offers an example of how to use corpus linguistics tools for privacy-related discourse analysis.

The articles assembled in this thematic issue on the politics of privacy show the diverse sites and often unexpected dimensions of societal struggle over control of data. By means of theoretical debate and empirical analysis they illustrate that and how the challenges and changes related to privacy set a political stage. Not least, the Covid-19 pandemic—as we are writing this editorial in June of 2020—has provided another, new and surprising, context for privacy research and for this volume. State-corporate surveillance aimed at hampering the virus' spread or radical datafication of family, education and work environments aiming at physical distancing have highlighted privacy as a critical issue for which a final definition remains open. Thus, in this sense, our collection offers various and nuanced accounts on privacy, its diverse realizations and contexts. Researching the politics of privacy in communication and media studies is obviously just about to start.

## Acknowledgments

Several contributions to this thematic issue were presented during a workshop entitled *The Politics of Privacy* in Mainz (Germany) in December 2019. We thank the Johannes Gutenberg University in Mainz for their generous support of the workshop and the ECREA Communication and Democracy section for their patronage. Judith E. Möller acknowledges personal funding from the Nederlandse Organisatievoor Wetenschappelijk Onderzoek (NWO Veni Grant, project nr. 191S.089).

## Conflict of Interests

The authors declare no conflict of interests.

## References

Barry, A. (2002). The anti-political economy. *Economy and Society*, *31*(2), 268–284.

Bentele, G., & Nothhaft, H. (2010). Strategic communication and the public sphere from a European perspective. *International Journal of Strategic Communication*, *4*(2), 93–116.

Birchall, C. (2016). Managing secrecy. *International Journal of Communication*, *10*(2016), 152–163.

boyd, d. (2012). Networked privacy. *Surveillance & Society*, 10(3/4), 348–350.

Cukier, K., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, *92*(3), 28–40.

Dean, J. (2005). Communicative capitalism: Circulation and the foreclosure of politics. *Cultural Politics*, *1*(1), 51–74.

Heikkilä, H. (2020). Beyond moral coupling: Analysing politics of privacy in the era of surveillance. *Media and Communication*, *8*(2), 248–257.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2017). Digital citizenship and surveillance. *International Journal of Communication*, *11*(2017), 731–739.

Igo, S. E. (2018). *The known citizen: A history of privacy in modern America*. Cambridge, MA: Harvard University Press.

Kannengießer, S. (2019). Reflecting and acting on datafication: CryptoParties as an example of re-active data activism. *Convergence: The International Journal of Research into New Media Technologies*. Advance online publication. https://doi.org/10.1177/1354856519893357

Livingstone, S. (2015). Active audiences? The debate progresses but is far from resolved. *Communication Theory*, *25*(4), 439–446.

Lokot, T. (2020). Data subjects vs. people's data: Competing discourses of privacy and power in modern Russia. *Media and Communication*, *8*(2), 314–322.

Lyon, D. (2018). *The culture of surveillance*: *Watching as a way of life*. Cambridge: Polity Press.

Madianou, M., & Miller, D. (2012). *Migration and new media: Transnational families and polymedia*. London: Routledge.

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

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269.

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

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication*, *8*(2), 291–301.

Möller, J. E., & Dogruel, L. (2020). Localizing the politics of privacy in communication and media research. *Media and Communication*, *8*(2), 237–247.

Möller, J. E., & Nowak, J. (2018). Surveillance and privacy as emerging issues in communication and media studies: An introduction. *Mediatization Studies*, *2*(2018), 7–15.

Munn, L. (2020). Staying at the edge of privacy: Edge computing and impersonal extraction. *Media and Communication*, *8*(2), 270–279.

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

Stachyra, G. (2020). Reflections upon the privacy in the converged commercial radio: A case study of Royal Prank. *Media and Communication*, *8*(2), 280–290.

Stolle, D., Hooghe, M., & Micheletti, M. (2005). Politics in the supermarket: Political consumerism as a form of political participation. *International Political Science Review*, *26*(3), 245–269.

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

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Wojtkowski, L., Brodzińska-Mirowska, B., & Seklecka, A. (2020). Polish privacy media discourse: Privacy as imposed policies. *Media and Communication*, *8*(2), 302–313.

**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

**Jakub Nowak** is an Associate Professor in the Institute of Social Communication and Media Studies at Maria Curie-Skłodowska University in Lublin, Poland. His research interests include political, cultural, and social aspects of digital technologies. https://orcid.org/0000-0002-5841-4404

**Sigrid Kannengießer** is a Guest Professor for Media and Communication Studies with a focus on media society at the Center for Media, Communication and Information Research at the University of Bremen, Germany. Her research focus is on media practices which critically reflect digitization and datafication processes, digital media and sustainability, transcultural and political communication, social movements, and gender media studies. https://orcid.org/0000-0002-2342-9868

**Judith E. Möller** is a Tenured Assistant Professor for Political Communication at the Department of Communication Science at the University of Amsterdam. She is affiliated with the Amsterdam School of Communication Research, the Center for Politics and Communication, and the Information, Communication, and the Data Society Initiative. In her research, she focuses on the effects of political communication, in particular social and digital media. She is fascinated by the complex relationship between expressions of citizenship and communication characterized by intertwined causal links and conditioned by the political system. https://orcid.org/0000-0001-7491-1155

COGITATIO

**Media and Communication (ISSN: 2183–2439)**
**2020, Volume 8, Issue 2, Pages 237–247**
**DOI: 10.17645/mac.v8i2.2869**

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

Submitted: 3 February 2020 | Accepted: 24 April 2020 | Published: 23 June 2020

**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.

**Keywords**
media research; politics; privacy; technology

**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 infrastructure 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

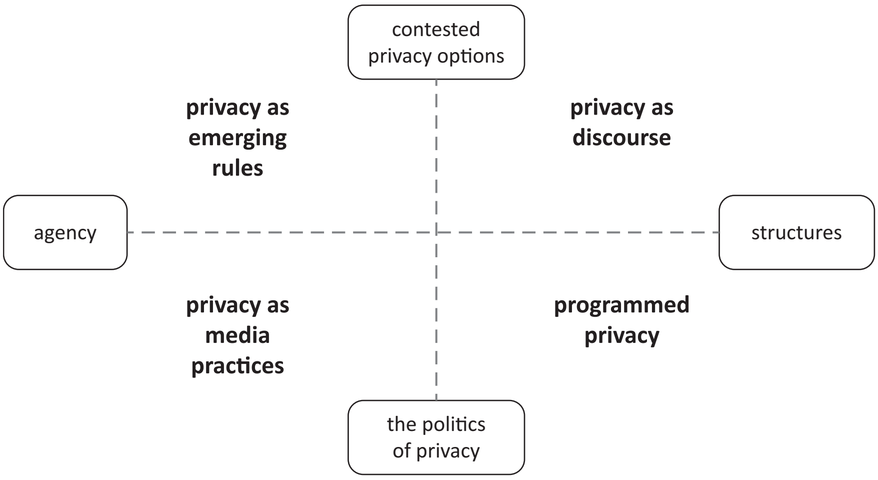


**Figure 1.** Four perspectives on the political implications of privacy.

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.

## Acknowledgments

We thank two anonymous reviewers for their valuable comments that helped refine the arguments in our article.

## Conflict of Interests

The authors declare no conflict of interests.

## 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 management: 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

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 2, Pages 248–257
DOI: 10.17645/mac.v8i2.2875

Article

# Beyond Moral Coupling: Analysing Politics of Privacy in the Era of Surveillance

Heikki Heikkilä

Faculty of Information, Technology and Communication, Tampere University, 33014 Tampere, Finland;
E-Mail: heikki.heikkila@tuni.fi

Submitted: 6 February 2020 | Accepted: 14 April 2020 | Published: 23 June 2020

**Abstract**

The article calls into question the prevailing discursive construction in contemporary debate on privacy and surveillance. At the core of this discourse is a moral coupling wherein surveillance is perceived as enemy and privacy as friend. Even if this binary approach renders arguments for democratising data more persuasive, a political cost accompanies it. As this discourse situates political struggle at the level of digital infrastructure and political structures, the moral coupling largely overlooks the ambiguities of how people in their various activities in a digital environment experience surveillance and privacy. Such a framing may discourage users at large from engagement with politics of privacy. Edward Snowden's autobiography is taken as a prominent example of the prevailing discourse. While analysing Snowden's descriptions of privacy and surveillance critically, the author points out the specific value of life stories in describing what privacy means and why it matters. While we cannot assume all people to be equally capable of considering how their own life intersects with the history of their society, we can presume that varying life stories should contribute to the public knowledge of privacy. To provide the framework necessary for appropriately contextualising empirical evidence, the author presents a model wherein privacy is composed of five dimensions: solitude, anonymity, secrecy, intimacy, and dignity.

**Keywords**

digital infrastructure; life-story research; online security; privacy; Snowden; surveillance

**Issue**

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

## 1. Introduction

In the last 15 years, the media environment has witnessed dramatic upheaval. The core of this change has been characterised as the Internet's metamorphosis from a loosely organised, decentralised, and pluralistic system into a tightly controlled, centralised, and commodified one under corporate and government control (Mosco, 2018, p. 210). While library shelves groan under the weight of books about what digital technology is doing to us and our world, many of the media's words about cloud computing, big data-based analysis, and the Internet of Things have been promotional or technically oriented (see Morozov, 2013). Simultaneously, burgeoning critical literature on surveillance is prompting discussion of what Mosco (2018, p. 213) terms "the serious policy issues that arise in a world of massive data centres, nonstop analysis of human behaviour and ubiquitous connectivity."

One of the key topics in critical debate over 'the next Internet' is digital surveillance and its reported effects on people's privacy. While this discussion features a host of perspectives, rooted in fields from social and legal theory to sociology or science and technology studies, I would argue that great centripetal force in media and political debate gets imposed via moral coupling of surveillance and privacy. The associated discourse tends to take a liberal, rights-oriented approach to privacy and proceed to ask institutions of surveillance “what hidden misuses, what unintended evils…you perpetuate behind your promises of safety” (Hong, 2017, p. 190). At least implicitly, this moral coupling presents surveillance as ‘bad’ or ‘evil’ while privacy gets portrayed as a desirable quality (Fuchs, 2011, p. 221), or as ‘friend.’

There is much to be said in favour of this moral-coupling discourse. It is instrumental in creating hermeneutics of suspicion around surveillance, thereby supporting political struggle to democratise data power and address worries about possible detrimental effects of digital surveillance on the public (Kennedy & Moss, 2015). In consequence, now “the future of state surveillance [appears] a little less certain, a little more open for negotiation” (Hong, 2017, p. 188). In the process, however, the discourse compromises conceptual depth. Said critique is not easily reconciled with the acknowledged benefits of surveillance in producing valuable knowledge about the population (Foucault, 2004), or in mitigating the ontological insecurity of modernity (Bauman & Lyon, 2013, p. 102). In the absence of theoretical reflexivity, this discourse skims over nuance and sometimes appears too dogmatic.

Simultaneously, with its dependence on a rights-based approach to privacy, the moral-coupling-based discourse is rather unresponsive to theories wherein privacy is relational and contextual (see boyd, 2014; Nissenbaum, 2004). Hence, the dominant discourse fails to engage with specifics of what people do in and with their privacy and how their lives may (or may not) be harmed by surveillance.

A further deficiency with this coupling lies in the political realm. As legal theorist Daniel Solove (2011, p. 2) notes, security interests—often cited in appeals for surveillance—are readily understood, for life and limb are at stake, while privacy rights remain abstract and vague. In such settings, the concepts are positioned in a hierarchy rather than balance, and the political efficacy of the respective arguments follows the same lines. While state surveillance institutions may be more readily subject to criticism amid the fallout from Edward Snowden’s revelations, any effect on intelligence legislation has been quite limited (on the UK’s situation, see Hintz & Dencik, 2017; on France, see Baisnée & Nicholas, 2017).

In addition, the moral-coupling discourse situates political struggle at structural level, highlighting roles of technological infrastructure elements and the big players managing these: principally, the most powerful state actors (the US, China, and Russia) and (mostly US-based) Internet behemoths such as Google, Amazon, and Facebook. In so doing, it largely overlooks the ambiguities of how people in their varied activities in digital environments experience surveillance and privacy. This framing has implications for public understanding of what is at stake in ‘the politics of privacy’ and may actually discourage users at large from political engagement.

Hence, it seems that the moral-coupling discourse, while representing necessary criticism of surveillance, is inadequate. Hong suggests that, for an escape from this predicament, a more robust form of surveillance criticism should reveal privacy to be a fragile and conflict-laden concept (Hong, 2017, p. 192). As tempting as that may sound, I set off in the opposite direction for my recommendation in this article. Given that a vast array of digital surveillance may be reshaping our lives, we must direct more theoretical and empirical effort, not less, to understanding people’s life-worlds.

The resulting empirical evidence of people’s thoughts on these matters or even of underlying reality would be meaningless without an accompanying pertinent theoretical perspective and research design to inform enquiry (Crotty, 1998, pp. 2–3). Accordingly, this article discusses both aspects: the concept of privacy itself and methodology. The theory-oriented aim for the article is, hence, a two-pronged one, which I pursue not by mapping out all relevant theories of privacy but by outlining a coherent typology of privacy that lends itself to empirical endeavours. While the main focus here is on the typology, I discuss the life story’s value for privacy studies alongside this. To that end, Snowden’s autobiography *Permanent Record* (2019) serves two functions. On the one hand, it exemplifies the moral-coupling discourse; on the other hand, it also provides hints of how to progress beyond it.

## 2. Surveillance as Enemy

In its contemporary context, the moral-coupling discourse refers most prominently to the US, with the most well-known recent disclosure of mass surveillance programmes pointing a finger at the US National Security Agency. Also, as the scale and scope of surveillance of users online has been revealed, it is large US-based companies that have come under the strongest public scrutiny. For the most part, the ensuing political debate on the subject has been structured by liberal political thought. Though the debate’s US political context is in many ways unique, the attendant moral-coupling discourse has found its way to European politics and media.

Snowden is a prominent figure in surveillance-related debates. In his autobiography, he vividly describes his path to learning of the secret mass-surveillance programmes developed and conducted by US intelligence agencies and to gradually growing convinced that those activities had to be revealed to the public, whatever the ensuing damage to his personal life. While the book shows that Snowden’s role in this exposure relied on exceptional technological skills, developed from early in life, the book is aimed, more than anything else, at justifying his central political conclusion: Surveillance in the hands of intelligence agencies had deviated from course and must be subject to proper democratic oversight.

Ever since his revelations pertaining to the NSA and other agencies, Snowden has been an important and controversial figure in international politics. Therefore, his autobiography is not just any life story. While the book was carefully designed to be a best seller for large global audiences, its format enables not only Snowden but also readers to "view the intersection of the life history of men with the history of their society, thereby enabling us to understand better the choices, contingencies and options open to the individual" (Robert Bogdan, as cited in Plummer, 2001).

Snowden (2019, p. 228) presents an occasion, less than a year prior to Snowden's revelations, that constituted a moment of epiphany of the sort cited as typical of autobiographies (Denzin, 1989):

> I picked up [the US Constitution] in earnest. I hadn't really read the whole thing in quite a few years, though I was glad to note that I still knew the preamble by heart. Now, however, I read through it in its entirety, from the Articles to the Amendments. I was surprised to be reminded that fully 50 percent of the Bill of Rights, the document's first ten amendments, were intended to make the job of law enforcement harder.

His view on that foundational law reveal Snowden's civil libertarian leanings, which tie in with the traditions of American political thought. This background aids in recognising that Snowden does not find surveillance bad by default. The problem resides, rather, in surveillance powers having overstepped the checks and balances of democratic governance. Besides the absence of effective systematic oversight, Snowden notes that intelligence activities are no longer truly in the state's hands: Much of the technological expertise is outsourced to private companies and individual system specialists more interested in sizeable pay packets than in the security of the nation. He concludes that, in consequence, digital surveillance has become dangerous, especially when under state auspices, and that there is urgent need for an appropriate political design placing those powers back in check.

In academic literature, the notion of surveillance as enemy is promulgated in empirical and theoretical contexts alike. Empirical studies have been undertaken to shed light on the actual mechanics and ultimate goals related to various surveillance agencies' data-gathering endeavours, profiling, and efforts to follow their targets across as many geographical locations and devices as possible (Morozov, 2013; Turow, 2011). For instance, ethnographic studies conducted in the US (Eubanks, 2018; Madden, Gillman, Levy, & Marwick, 2017) and the UK (Redden, Dencik, & Warne, 2020) attest to how algorithmic surveillance is growing into an indispensable tool for the public sector, most notably in social work and policing.

The main conclusion from the empirical studies is that surveillance in the digital environment is expansive, if not excessive. Critical theorists tend to go even further by claiming that surveillance is, above all, a transformative force. In her discussion of 'surveillance capitalism,' Zuboff (2019, p. 93) argues that the economic market's prevailing logic has changed, declaring that "now serving the genuine needs of people is less lucrative, and therefore less important, than selling predictions of their behavior." Couldry and Mejias (2018), in turn, posit that datafication enables appropriation of all life as raw material for economic exploitation in precisely the ways colonialism enabled appropriating land, resources, and bodies for European rulers' benefit in the eighteenth and nineteenth century.

Whether presented against the backdrop of the Constitution, capitalism-related critical theory, or critique of colonialism, surveillance poses threats to democratic governance. Accordingly, it seems reasonable to assume that surveillance is at least potentially 'bad' or 'evil,' thereby warranting politicisation as 'enemy.' A question remains, though, as to whether this picture is comprehensive enough. Does knowing the enemy mean that we also know the friend?

## 3. 'Privacy' as an Empty Word

With the moral-coupling discourse, surveillance theorists tend to discuss privacy in a narrow sense of the concept. For instance, Zuboff (2019, p. 90) argues that privacy has been not eroded but, as a decisional right, redistributed as surveillance capital; that is, decisions about what to reveal or keep secret are no longer made by individual users, as companies have gained those rights and exercise them by appealing to dubious terms of service. With this stance, her research, while focused on surveillance, covers privacy too. After all, the former has subsumed the latter. Where Zuboff addresses decisional privacy only insofar as it refers to content and data generated by users on digital platforms, others extend the consideration of decisional privacy to matters of lifestyle and the life projects one pursues, as with issues of which church to attend or what education to pursue (Rössler, 2005, p. 79).

Within the moral coupling discourse, limited interest in the concept of privacy is not troubling, as the expansion of surveillance is wrong in its own right, violating such key values of liberal democracy as transparency. For example, in book *The Black Box Society*, Pasquale (2015) argues that people do not comprehend the extent of the information collected through close monitoring by governmental and other institutions, let alone how it is used or the consequences of that collection. The problem is not that people lose their privacy but that their right to know is not respected.

While it may be surprising, then, that Snowden writes at length about privacy, there is a stark contrast against his explicit indictment of state surveillance. His defence of privacy remains abstract and elusive. The autobiography makes this rather explicit (2019, p. 208): "The word 'privacy' itself is somewhat empty, because it is essentially indefinable, or over-definable. Each of us has our own idea of what it is. 'Privacy' means something to everyone. There is no one to whom it means nothing."

Snowden draws from a negative definition of privacy, one referring to absence of intervention and thus leaving the space relatively empty. That said, ripples from that space are far from absent, for privacy as a right constitutes a foundation to all liberties. Even if Snowden talks about subjects granted privacy in the plural (‘Americans’), the emphasis is on the individual and an ideal figure of the autonomous liberal subject:

> Americans only have a ‘right’ to free speech because the government is forbidden from making any law restricting that freedom, and a ‘right’ to a free press because the government is forbidden from making any law to abridge it. They only have a ‘right’ to worship freely because the government is forbidden from making any law respecting an establishment of religion, and a ‘right’ to peaceably assemble and protest because the government is forbidden from making any law that says they can’t. (Snowden, 2019, p. 207)

By claiming that privacy is indefinable and over-definable at the same time, Snowden points to what limits empirically understanding privacy. He suggests, on the one hand, that privacy is so abstract that a proper definition of the concept is beyond his grasp; on the other hand, he simultaneously anchors it in concrete subjective experiences and individuals’ choices (either way, any further analysis or theorising that might be possible lies outside his interest here). While the book refers to many concrete moments in which experiences of privacy were particularly meaningful for Snowden—among the positive ones are moments of intimacy experienced both offline and online (2019, pp. 99–100), alongside opportunities for time alone while commuting (p. 108)—he otherwise prefers to talk about privacy in generic rather than personal terms. For instance, in relation to one’s autonomy and dignity, he states “you don’t have to be a closet fetishist to have done things that embarrass you and to fear that strangers might misunderstand you if those things were exposed” (p. 95).

In Snowden’s life story, moral coupling of surveillance with privacy contributes to a narrative of growth toward politically consistent subjectivity. The story presents strict adherence to two central tenets of liberal (if not libertarian) democracy: a belief in privacy as the foundation of all personal liberties and trust in the system of checks and balances in preventing abuse of power. This idealistic, textbook-type formulation is cast in sharp relief against an atmosphere of pervasive surveillance realism aimed at normalising surveillance infrastructure (Dencik, 2018, p. 31). The contrast highlights Snowden’s separation from the institutions to which he pledged loyalty once upon a time, and his choice of the former over the latter articulates a difference from his erstwhile colleagues in the intelligence community, presumably more compliant with surveillance realism.

While describing some of his own private moments in the book, Snowden says little about lives of people outside his closest circle. Hence, the reader is shown a life-world that, apart from his brief stint in Japan and associations with manga fans, is populated by white Anglo-Saxon civil servants. More importantly, Snowden’s portrayal does not overtly connect with lives of people showing less interest in and knowledge of digital systems and surveillance. My point here is not to point a finger at any lack of cultural diversity in Snowden’s account so much as highlight possible connections with how surveillance and privacy get coupled in a narrative from this perspective.

On our journey beyond such moral coupling discourse, we can ask what sorts of evidence and voices get overlooked through it. With the discussion below, I issue a challenge to broaden the perspective by overcoming the moral-coupling discourse’s limited, outdated understanding of users in a digital environment. However normatively commendable Snowden’s perspective may be, it is tied to a specific understanding of the politics of privacy that is not merely specific but also exclusive.

## 4. Surveillance from Users’ Perspective

Critical debate on surveillance has a cumulative effect on the moral coupling in that the more information about the scope of surveillance is revealed, the more likely it is for surveillance to be perceived as the enemy. Still, studies among users suggest that user attitudes toward surveillance are often contradictory, even paradoxical. Surveys frequently identify a gulf between user-expressed attitudes and behaviour. Empirical findings indicate that, while users are concerned about their privacy on the Internet in general, and within the social web in particular, usage behaviour does not reflect these concerns correspondingly (CIGI–Ipsos, 2017). Two main factors are cited as behind this privacy paradox: Users reportedly lack awareness of opportunities to protect their privacy, and they tend to underestimate the privacy dangers of self-disclosure (Taddicken, 2014, pp. 248–249).

The privacy paradox and its part in explaining users’ relationship to surveillance constitutes a controversial topic in studies of science, technology, and society. Criticisms aside (see boyd & Hargittai, 2010; Tufekci, 2008), the interpretation predominating in surveys is that discrepancies between attitudes and informed actions reflect shortcomings in rationality among users, suggesting that users are unwittingly compliant with surveillance forces that may abuse them (Barth & de Jong, 2017, pp. 1038–1040). This view is consistent with the moral coupling: with people being only partially committed to the idea that surveillance is the enemy and that privacy must be safeguarded, greater education of the public in the hazards of surveillance and in means of defending one’s privacy is required. In some cases, the moral-coupling discourse adopts a false-consciousness framework as a foundation for efforts to explain why subjects accept surveillance in an act of ‘voluntary servitude’ (Robert Pallitto, as quoted in Hong, 2017, p. 189).

This reasoning is problematic, not least because it operates with vague analytical categories such as ‘attitudes' and 'behaviour' and draws broad generalisations about them without accounting for the everyday contexts in which uses of social media and the Internet are embedded. At least implicitly, research into the privacy paradox seems to rely on assumptions dating from the mass-communication-dominated era, when media consumption was perceived as introspective; e.g., in his classic study of newspaper-reading, Berelson (1949, p. 199) noted that readers value newspapers for respite functions, as reading 'provides a vacation from personal care by transporting the reader outside his own immediate world.'

Even if respite may be found in media on digital platforms too, this environment tends to facilitate and contribute to encounters involving interaction rather more than introspection. The digital landscape affords activity that can be social while still technical. It enables encounters with "all friends, relatives, teachers, neighbors and many unknown others" (Meyrowitz, 1985, p. 4) via interaction involving much more: numerous functions of computers, as hardware and software, local and remote, respond to every keystroke and mouse movement (Manovich, 2001, p. 155). An appropriate metaphor for the digital landscape is traffic congestion. Users cannot control everything and may recognise this, expecting to be interrupted (or even disturbed) by other users and 'third parties' such as advertisers and infrastructural elements.

Various forms of disturbance online can be readily experienced as surveillance. When official surveillance is associated with situations of social interaction, users tend to deem the matter serious. Among more commonplace cases are incidents of stalking, webcam-based blackmail, blackmail-related scams, and 'sextortion,' in which the actors responsible are usually peer users, not public institutions or commercial entities (Heikkilä, 2018, pp. 68–69). In more everyday activities, users are reminded of surveillance through technical interaction such as automated, algorithm-governed 'communication' that can be generated whenever users purchase goods/services online, participate in customer-loyalty programmes, use online search engines, click on advertisements, upload content to social-media platforms, or sign in to other services via a personal Google ID or Facebook account (Kennedy, 2018).

In day-to-day life, awareness of practices in that last class tends to fade into the background, getting reactivated when clearly surveillance-based feedback reaches the user. Many institutions responsible for surveillance, such as intelligence agencies and the police, deliberately avoid feedback loops, since informing/reminding of surveillance would go against their interests. In the meantime, commercial Internet service providers apply surveillance feedback loops differently, as their business model is predicated on the idea that all advertising must be targeted (Turow, 2013). Therefore, nearly every piece of empirical evidence of surveillance that users see is advertising. All the rest is left to the imagination.

While outputs in selective surveillance feedback loops frequently elicit reactions from users, these are not always interpreted as representing invasions of privacy. Depending on how well the cues calculated by algorithmic systems mesh with users' instantaneous preferences, an automated message may be either pleasing and relevant or disturbing and unsuccessful (Ruckenstein & Granroth, 2019). Users may feel angry when Facebook overtly monetises their personal data (Skeggs & Yuill, 2016, p. 387) and experience 'strange sensations' (Bucher, 2017, p. 35) when seeing evidence of their actions' exposure to outside surveillants—e.g., immediately after loading a friend's Facebook profile, seeing that friend in one's Facebook News Feed.

While users in Ruckenstein and Granroth's (2019) study did not know how Facebook's or Google's proprietary algorithms operate, they recognised the workings of algorithms online. Interviewees proved well versed in surveillance and privacy issues, mainly through everyday understandings of algorithms as shaped by what is taught in schools, discussion with friends, and the media. These observations reveal that, while users hold contradictory attitudes to surveillance and privacy, this phenomenon stems not from lack of awareness/knowledge but from experiences of banality, a concept referring (per Lehmuskallio, Heikkilä, & Kortesoja, 2018), to non-distinctive, ordinary, dull, and clichéd parts of our digitally enhanced life.

While this perspective does not imply surveillance being 'bad' by default, it does point to banality as an indirect consequence of surveillance. Surveillance implies certain structures that impose social order, structures that cannot be willed away. That consequence is daunting, in that banality tends to undermine the very qualities that the moral-coupling discourse is employed to encourage: moral and political reflexivity surrounding the effects of surveillance (see Arendt, 1958).

## 5. Pursuing Meaningful Analysis of Privacy

Liberally oriented theory characterises privacy as a right or an individual's choice. As a right, privacy constitutes a circle around every individual, "which no government…ought to be permitted to overstep…and within which that person ought to reign uncontrolled either by any other individual or by the public collectively" (Mill, 1965, p. 938). The second liberal framing defines privacy as a claim of individuals' stake for determining when, how, and to what extent information about them is communicated to others (Westin, 1967, p. 7). Both ideas abstract from issues related to political economy of capitalism, such as exploitation and income/wealth inequality (Fuchs, 2011, p. 226). In so doing, they do not merely ignore the fact that neither rights to privacy nor opportunities to control one's personal information are equally distributed. As studies on the uses of data-profiling and algorithmic analysis of underprivileged neighbourhoods and social groups suggest, one's resources for establishing and maintaining privacy depend on a combination of sociological variables, such as race, income, and gender (Eubanks, 2018; Gangadharan, 2012).

Liberal theories of privacy vary with regard to the elasticity of the private realm articulated. In rights-based versions, privacy is an ethical imperative so should exist relatively independently of human actions. For choice-based theories, privacy depends on individuals' behaviour, which renders it variable, dynamic, and flexible. In relational theories of privacy, both rights and choices are subject to context-bound interpersonal negotiation. Communication privacy management theory is a school of research that undertakes analysis of how people make decisions about revealing or concealing information they consider private (Petronio & Durham, 2015, p. 336). These scholars subscribe to microanalysis in the style of Goffman, whereby researchers observe an open-ended set of social negotiations over privacy norms. This research assignment should provide a basis for aggregating people's various expectations as to privacy. There is an obvious methodological problem with this strategy: Given that the number of social situations that people engage in is unbounded, the selection of situations submitted to empirical analysis must be likewise unbounded.

In another recommendable methodological strategy, privacy is conceived of as a condition. With this intermediate design, privacy could be approached as a cluster of related but mutually independent components. While there are numerous candidates for such a list (see Fuchs, 2011, pp. 222–224), I would begin with three categories suggested by legal theorist Raymond Wacks (2010, pp. 41–42): solitude, anonymity, and secrecy.

Solitude, sometimes referred to in the privacy literature as seclusion or retreat, involves a time and place wherein people can be unobserved and undisturbed by others (Rössler, 2005, p. 144). Moments of seclusion offer possibilities for stepping outside social events and populated surroundings to be alone. Solitude constitutes a space that other people cannot see for an individual's habits or routines. The value of solitude lies in its voluntary and temporary nature; where the condition is imposed and cannot be lifted, it produces loneliness, which people usually try to avoid. Unlike other dimensions of privacy, solitude is anchored in spatial settings, the spaces people tend to regard as the safest, such as one's home.

Anonymity, in turn, brings in the possibility of not standing out relative to others in the population. With anonymity, people may attend social events (public rallies etc.) without being recognised/identified, and it may encourage individuals to experiment with their identity. This may be a source of independence, as anonymous groups are difficult to control. There is a darker side too, since capacity for unidentified agency may be exercised irresponsibly (e.g., contemporary problems of uncivil behaviour on online discussion boards are strongly linked to anonymity). However, anonymity can entail lack of power, because anonymous people are not fully visible to each other even if they may engage in the same practice or activity. A well-known example is visible in traditional media audiences (viewers and readers), who have limited capacities to make themselves heard and influence media production (Ang, 1991; Heikkilä, 2018, p. 70).

Finally, secrecy is a characteristic of interpersonal communication arising among selected persons while hidden from others. In close interpersonal relations, secrecy and trust are mutually constitutive elements, depending upon and strengthening each other. Secrecy is significant for politics of privacy, and classic theories of the public sphere regard it as an essential precursor to citizenship in that political ideas tend to spring from non-public reflexivity. At the same time, secrecy also provides a veil for terrorist 'sleeper cells' or perpetrators of domestic violence.

From our discussion of Snowden's autobiography, we can see that secrecy is an important aspect of privacy for him. This view resonates with the Habermasian theory of the bourgeois public sphere, in which the emergence of rational publics depends on opportunities for wealthy men to reflect on current affairs in literary clubs, private homes, and coffee houses without interference from those in power. The same dynamics have been identified with regard to many other political movements, aimed at national independence, civil rights for minorities, equality for women, and sexual self-determination (Fraser, 1989). Outside his autobiography, Snowden rarely uses such words as 'citizenship' or 'politics.' He speaks more generally of 'liberty.' About a year after his most explosive revelations, he told interviewers that "reasonable people would grant that privacy is a function of liberty. If we get rid of privacy, we're making ourselves less free" ("Edward Snowden interview," 2014).

Snowden's view on privacy differs from that in algorithmic imaginaries of ordinary Internet users, who discuss their relations to digital surveillance almost exclusively from the perspective of anonymity (Bucher, 2017; Ruckenstein & Granroth, 2019). For them, privacy enables relative freedom of movement over the digital landscape, whereby their behaviour might be visible to third parties but their identities are not revealed. Thus, their access to online services and platforms comes with a cost but this involves negotiation, quite different from the bargaining related to secrecy or seclusion. At some point, these components do intersect, though, since much of targeted advertising relies on age-gender-location-based sorting categories. Therefore, young women are continually told about beauty products and pregnancy tests while young men are targets for dating-site ads and claims of 'hot singles near you.'

Outside the particular conditions considered, users in these and other groups may switch role (e.g., from citizen to consumer or vice versa) as the situation dictates. Nonetheless, even the brief analysis above demonstrates that privacy has multiple meanings and functions, which need to be taken into account for meaningful debate on surveillance and the politics of privacy. Because

**Table 1.** Dimensions of privacy.

| Dimension | Meaning | Functions | Threatened by… |
|---|---|---|---|
| Solitude | being unseen and unheard by others | tranquillity, relaxation | peer users, the Internet of Things |
| Anonymity | being non-distinctive among one's peers | agency without accountability | digital-market actors |
| Secrecy | strategic interpersonal communications | formation of opinions | the security state |
| Intimacy | sharing of emotional and/or physical proximity | showing love and devotion | accidental or deliberate 'peeping toms' |
| Dignity | absence of humiliation and embarrassment | self-esteem, mutual respect | peer users, digital-market actors |

Source: Adapted from Heikkilä (2018) and Wacks (2010).

these dimensions of privacy, or clusters, represent such valuable tools for analysing what privacy would mean as condition, it is worth looking at additional attributes mentioned in privacy studies, outside these categories, for further tools. To gain a fuller toolbox, I would add to the list, alongside seclusion, anonymity, and secrecy, at least two further categories: intimacy and dignity. All five dimensions of the resulting framework are shown in Table 1.

Intimacy involves communication and sharing of emotional and/or physical proximity with others, such as a spouse, child, or friend. Referring to a specific quality of close mutual connection and the process of building this (Jamieson, 2011), intimacy ties in with the positive human qualities of love and commitment. It also enables playfulness in the form of 'backstage language' and unedited conversation (Goffman, 1959, p. 128), which is instrumental to forging the connection but could lead to harm for the intimate partners if stripped of context and revealed to others. A historical figure symbolising threats to intimate privacy is Peeping Tom, whose role was at some point adopted by tabloid journalists and paparazzi. Recent important developments in cameras, drones, and other devices have put the same techniques at anyone's disposal (Andrejevic & Burdon, 2015; Koskela, 2011).

Finally, dignity involves self-respect and reputation, which point to conditions that, while within the innermost self, are taken on and maintained intersubjectively (Honneth, 1995). Dignity is grounded in cultural norms of behaviour or 'good manners.' Hence, codes of dignity are contingent, not universal. The value of dignity is revealed when it is breached—when someone feels embarrassed or humiliated by disclosure of deeds or thoughts that were not intended for sharing with others (Margalit, 1996).

Only this dimension of privacy does not involve a specific mode of 'doing' that one would purposefully pursue for privacy. Rather, dignity involves a state of mind, which may be aggregated from other aspects of privacy though dignity does not necessarily require all of the other conditions to be met. An elderly person dependent on constant professional assistance from nurses or social workers may feel dignified even if opportunities for solitude, anonymity, secrecy, or intimacy are greatly compromised. Given that dignity is a state of mind, it is dependent on one's personal psychological resilience. In addition, it seems that dignity is the facet of privacy least easily restored after undermining.

## 6. Conclusion

With this article, I have challenged a discursive construction that permeates much of contemporary debate on privacy and surveillance, a discourse at whose core is moral coupling wherein surveillance is taken as an enemy and privacy as a friend. While this discourse is widespread in news media and finds support in considerable recent critical surveillance literature, it proved particularly fruitful to problematise it by considering Snowden and his autobiography as exemplars of this line of thought.

Although he and other critics of surveillance contribute to public knowledge of digital surveillance in numerous ways, they, at the same time, seem remarkably indifferent to the fact that Internet users in general are not similarly outspoken critics of surveillance. Additionally, surveillance critics demonstrate limited interest in delving into conceptual analysis of privacy. Might there be something more concrete or nuanced than an 'empty' word, a 'no-go zone,' or an abstract right?

While privacy has elicited interest within many fields of research, the concept has also frustrated many. In the course of listing several typologies and taxonomies of privacy, Fuchs (2011, p. 222) notes a key problem with privacy typologies in that they are arbitrary: "There is no theoretical criterion used for distinguishing the differences between the categories." For Hong (2017, pp. 191–192), privacy is too fragile and contradiction-rife a concept to employ for countering the growth of surveillance. These arguments are warranted but, in my view, they should not distract us from examining what people do in and with their privacy.

Therefore, in this article, I have attempted to conceptualise privacy as a condition of being in which five dimensions may be distinguished for purposes of analysis. The term 'being,' again, has a double meaning: It pertains to situations wherein people decide on revealing/concealing information that they consider private, and it also denotes people's sociologically varying situations in life. It remains for empirical studies to shed light on how, if at all, the meaning of privacy differs with what people do in and with privacy and uncover any contingency on whether they are male or female, rich or poor, residents of a mansion or a shack. This awareness is crucial for extending studies of privacy beyond the abstract standard citizen found in so many textbooks and legislative documents. Moving from discussions about privacy as right to work on privacy as condition is a huge first step, even if the setting remains the context of Western societies. Shifting still further would call for even more profound rethinking both theoretically and methodologically.

In this endeavour, fittingly enough, Snowden's autobiography may be transformed from a theoretical problem into a methodological solution. It holds value in not merely setting forth an authorised stakeholder's view on one of the most important political processes of the last decade but also employing the life story as its format. Thereby, readers can view the intersection of an individual's life history with the history of society. This story is open to multiple analytical readings, and our brief analysis of Snowden's relations to surveillance and privacy provides only a taste of the potential of the approach. The next move on the path would be to locate life stories that decisively differ from Snowden's.

Life-history research, of course, has its own life, dating back to the Chicago School of Sociology in the early 20th century and still further (Plummer, 2001). This methodology has been applied to feminist surveillance studies (see Dubrofsky & Magnet, 2015). Since the rich methodological insights developed within that research tradition cannot be discussed here in detail, I refer only to Marwick and boyd (2018), who highlight the value in advancing research into privacy at the margins. The stark reality is that achieving privacy is especially difficult for those who already are otherwise marginalised. They emphasise: "Parents argue that they have the right to surveil their children 'for safety reasons.' Activists who challenge repressive regimes are regularly monitored by state actors. And poor people find themselves forced to provide information in return for basic services" (Marwick & boyd, 2018, p. 1158).

It seems that if we want to know more about privacy and how surveillance reshapes privacy, there is much to learn from people for whom privacy is a distinctly scarce resource, those who work hardest to maintain what is left of it.

Studies of privacy-related vulnerability would guide us toward hearing and heeding the life stories of people with experiences of discriminatory surveillance practices, such as redlining and profiling of whatever sort, be it racial, medical, or political (Eubanks, 2018; Gangadharan, 2012; Redden et al., 2020). This is not to say that only experiences of the underprivileged matter but, rather, to suggest that this form of knowledge is essential for dealing with politics of privacy.

## Acknowledgments

This article is based on research conducted in the Banal Surveillance research project (2018–2022), funded by the Academy of Finland. The author wishes to thank the two anonymous reviewers for their comments. I am grateful also for feedback from Anna Shefl, Minna Saariketo, and my IASR colleagues Laura Ahva, Risto Heiskala, Mervi Kaukko, Hanna Ojala, and Saara Pellander.

## Conflict of Interests

The author declares no conflict of interests.

## References

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television & New Media*, *16*(1), 19–36.

Ang, I. (1991). *Desperately seeking the audience*. London: Routledge.

Arendt, H. (1958). *Eichmann in Jerusalem: A report on the banality of evil*. New York, NY: Viking Press.

Baisnée, O., & Nicholas, F. (2017). Security, terror and freedom: The dynamics of public opinion in the French surveillance debate. In R. Kunelius, H. Heikkilä, A. Russell, & D. Yagodin (Eds.), *Journalism and the NSA revelations: Privacy, security and the press* (pp. 91–112). London: IB Tauris and Reuters Institute for the Study of Journalism.

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

Bauman, Z., & Lyon, S. (2013). *Liquid surveillance: A conversation*. Cambridge: Polity.

Berelson, B. (1949). What 'missing the newspaper' means. In P. Lazarsfeldt & F. Stanton (Eds.), *Communication research 1948–1949* (pp. 111–128). New York, NY: Harper & Brothers.

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

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8), 1–23.

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, *20*(1), 30–44.

CIGI–Ipsos. (2017). 2017 CIGI–Ipsos global survey on Internet security and trust. *CIGI Online*. Retrieved from http://www.cigionline.org/internet-survey-2017

Couldry, N., & Mejias, U. (2018). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4), 336–349.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in research process*. London: SAGE.

Dencik, L. (2018). Surveillance realism and the politics of imagination: Is there no alternative? *Krisis*, *1*(1), 31–43.

Denzin, N. (1989). *Interpretive biography*. London: SAGE.

Dubrofsky, R., & Magnet, S. A. (Eds.). (2015). *Feminist surveillance studies*. Durham, NC: Duke University Press.

Edward Snowden interview: The edited transcript. (2014, July 18). *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York, NY: St. Martin's Press.

Foucault, M. (2004). *Security, territory, population: Lectures at the Collège de France 1977–1978*. London: Palgrave Macmillan.

Fraser, N. (1989). *Unruly practices: Power, discourse, and gender in contemporary social theory*. Minneapolis, MN: University of Minnesota Press.

Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4), 220–237.

Gangadharan, S. (2012). Digital inclusion and data profiling. *First Monday*, *17*(5). https://doi.org/10.5210/fm.v17i5.3821

Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Doubleday.

Heikkilä, H. (2018). Privacy under surveillance: Towards a conceptual analysis of the price of connection. *Northern Lights*, *16*(1), 59–74.

Hintz, A., & Dencik, L. (2017). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, *5*(3), 1–16.

Hong, S. (2017). Criticizing surveillance and surveillance critique: Why privacy and humanism are necessary but not sufficient. *Surveillance & Society*, *15*(2), 187–203.

Honneth, A. (1995). *The struggle for recognition: The moral grammar of social conflicts*. Cambridge: Polity Press.

Jamieson, L. (2011). Intimacy as a concept: Explaining social change in the context of globalisation or another form of ethnocentricism? *Sociological Research Online*, *16*(4), 1–13.

Kennedy, H. (2018). Living with data: Aligning data studies and data activism through a focus on everyday experiences of datafication. *Krisis*, *1*(1), 18–30.

Kennedy, H., & Moss, G. (2015). Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society*, *2*(2). https://doi.org/10.1177/2053951715611145

Koskela, H. (2011). Hijackers and humble servants: Individuals as camwitnesses in contemporary controlwork. *Theoretical Criminology*, *15*(3), 269–282.

Lehmuskallio, A., Heikkilä, H., & Kortesoja, M. (2018). *Banal surveillance: An introduction to a framework of a study*. Paper presented at the Amsterdam Privacy Conference 2018, Amsterdam, The Netherlands.

Madden, M., Gillman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1), 53–125.

Manovich, L. (2001). *The language of new media*. Cambridge, MA: MIT Press.

Margalit, A. (1996). *The decent society*. Cambridge, MA: Harvard University Press.

Marwick, A., & boyd, d. (2018). Understanding privacy at the margins. *International Journal of Communication*, *12*, 1157–1165.

Meyrowitz, J. (1985). *No sense of place: The impact of electronic media on social behavior*. New York: Oxford University Press.

Mill, J. S. (1965). *Principles of political economy* (Vol. 2). London: University of Toronto Press.

Morozov, Y. (2013). *To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exist*. New York, NY: Public Affairs.

Mosco, V. (2018). A critical perspective on the post-Internet world. *Javnost: The Public*, *25*(1/2), 210–217.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Petronio, S., & Durham, W. (2015). Communication privacy management theory: Significance for interpersonal communication. In L. Baxter & D. Braithwaite (Eds.), *Engaging theories in interpersonal communication* (pp. 335–347). London: SAGE.

Plummer, K. (2001). *Documents of life 2: An invitation to critical humanities*. London: SAGE.

Redden, J., Dencik, L., & Warne, H. (2020). Datafied child welfare services: Unpacking politics, economics and power. *Policy Studies*. https://doi.org/10.1080/01442872.2020.1724928

Rössler, B. (2005). *The value of privacy*. Cambridge: Polity.

Ruckenstein, M., & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24.

Skeggs, B., & Yuill, S. (2016). Capital experimentation with person/a formation: How Facebook's monetization refigures the relationship between property, personhood and protest. *Information, Communication & Society*, *19*(3), 380–396.

Snowden, E. (2019). *Permanent record*. London: Macmillan.

Solove, D. (2011). *Nothing to hide: The false trade-off between security and privacy*, New Haven, CT: Yale University Press.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Assisted Communication*, *19*(2), 248–273.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36.

Turow, J. (2011). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press.

Turow, J. (2013). *The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power*. New Haven, CT: Yale University Press.

Wacks, R. (2010). *Privacy: A very short introduction*. Oxford: Oxford University Press.

Westin, A. (1967). *Privacy and freedom*. New York, NY: Altheneum.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: Public Affairs.

## About the Author

**Heikki Heikkilä** is Associate Professor in Journalism Studies at Tampere University (starting September 2020) and Senior Research Fellow at the Advanced Research Centre for Social Research (IASR). His research focuses on the effects of digitalisation on journalism and its (assumed) audiences. He is also written about surveillance and privacy. He is co-editor of the book *Journalism and the NSA Revelations: Privacy, Security and the Press* (IB Tauris, 2017, with Risto Kunelius, Adrienne Russell and Dmitry Yagodin), and he has published articles in *Journalism: Theory, Practice & Criticism*, *Digital Journalism*, *European Journal of Communication*, and *Javnost: The Public*.

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

Article

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

Philipp K. Masur

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

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

**Abstract**

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

**Keywords**

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

**Issue**

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

## 1. Introduction

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

Although concepts of privacy can be traced back to different schools of thought, contemporary discussions of online privacy almost exclusively adopt a perspective that is rooted in liberal theories (e.g., Hobbes, 1651; Mill, 1859/2015). In trying to grasp and describe current threats to privacy such as ubiquitous surveillance and large-scale data collection (Greenwald, 2014), the increasing commodification of information (Sevignani, 2016), the blurring of public and private in networked environments (Masur, 2018b), and the corresponding malleability of the individual by powerful economic players (Acquisti, Brandimarte, & Loewenstein, 2015), privacy scholars and the public alike conceive of privacy, in one way or the other, as a form of protection against social, economic, or institutional interferences. This perspective resembles the notion of 'negative freedom' (Berlin, 1969). Variants of such a negative conception of privacy can be found in non-intrusion theories of privacy (e.g., Warren & Brandeis, 1890), seclusion theories of privacy (e.g., Gavison, 1980; Westin, 1967), as well as in control and limitation theories of privacy (e.g., Altman, 1975; Miller, 1971; Rachels, 1975; Tavani, 2007).

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

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

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

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

The goal of this article is twofold. First, I discuss the role of online privacy literacy in providing individuals with the ability to protect themselves against external social, economic, and governmental influences (alluding to a negative privacy conception). In this regard, online privacy literacy plays an important role in democratic, but even more so in authoritarian societies, in which individuals may be more in need to protect themselves against identification. Second, I explore how societal change towards a more positive notion of privacy (i.e., informational self-determination) might be possible. The main argument is that again online privacy literacy—the often-proposed solution to protect people's privacy against external influences—may also provide the basis for social transformations because it motivates individuals to become agents of social change and to engage in acts of resistance. That said, this deliberation process may be limited to democratic societies in which social transformations through civic engagement are possible. In authoritarian regimes such safe avenues for public deliberation may not be feasible.

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

## 2. An Extended Model of Online Privacy Literacy

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

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

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

### *2.1. Factual Privacy Knowledge*

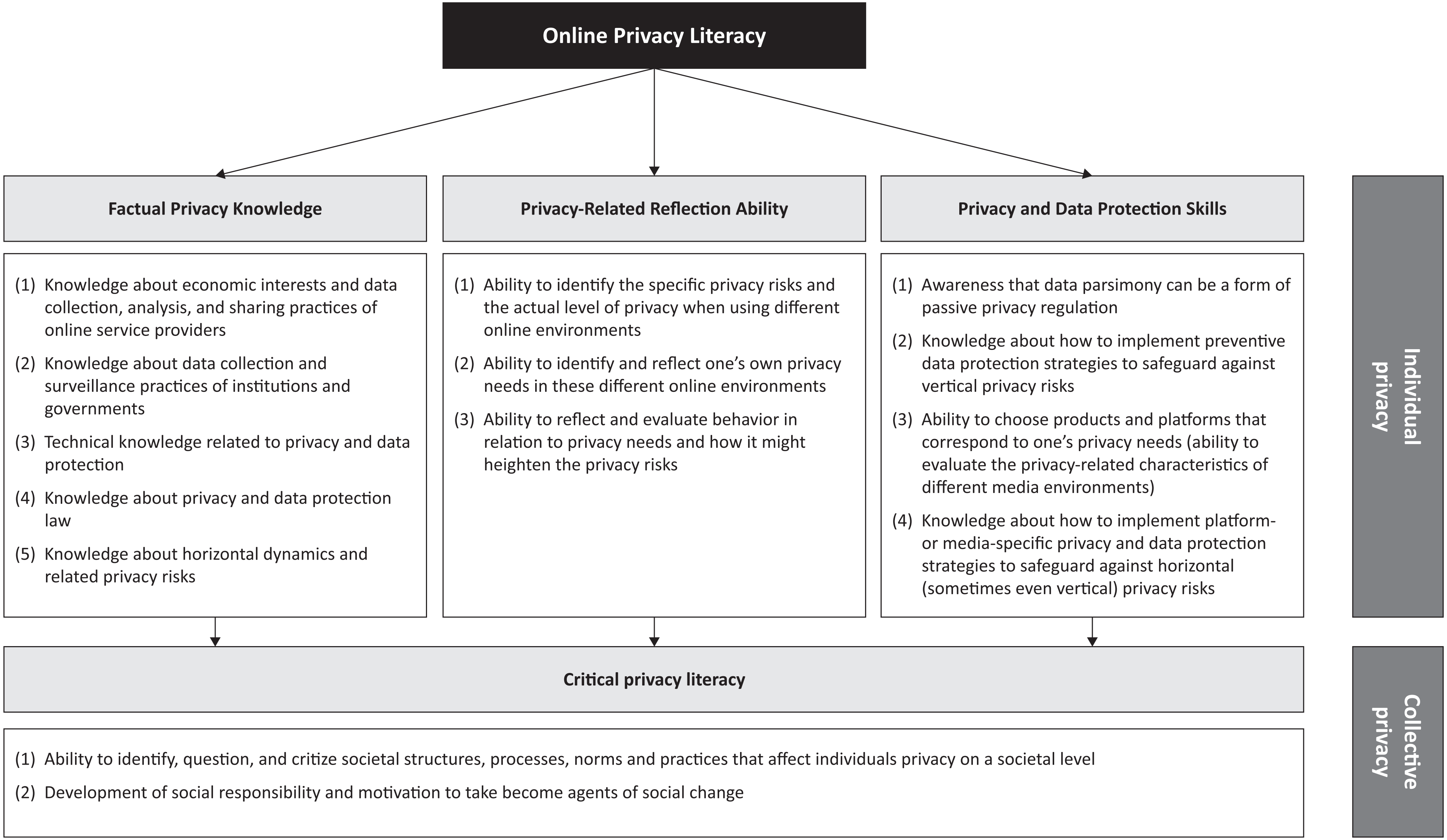
This dimension acknowledges that familiarity, awareness, and understanding of facts, concepts, information, and conditions is essential for developing any kind of literacy. Similarly to knowing what a computer looks like and knowing what it can be used for represents a first step towards developing the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

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

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

### *2.2. Privacy-Related (Self-)Reflection Ability*

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



Online Privacy Literacy

Factual Privacy Knowledge

(1) Knowledge about economic interests and data collection, analysis, and sharing practices of online service providers

(2) Knowledge about data collection and surveillance practices of institutions and governments

(3) Technical knowledge related to privacy and data protection

(4) Knowledge about privacy and data protection law

(5) Knowledge about horizontal dynamics and related privacy risks

Privacy-Related Reflection Ability

(1) Ability to identify the specific privacy risks and the actual level of privacy when using different online environments

(2) Ability to identify and reflect one's own privacy needs in these different online environments

(3) Ability to reflect and evaluate behavior in relation to privacy needs and how it might heighten the privacy risks

Privacy and Data Protection Skills

(1) Awareness that data parsimony can be a form of passive privacy regulation

(2) Knowledge about how to implement preventive data protection strategies to safeguard against vertical privacy risks

(3) Ability to choose products and platforms that correspond to one's privacy needs (ability to evaluate the privacy-related characteristics of different media environments)

(4) Knowledge about how to implement platform- or media-specific privacy and data protection strategies to safeguard against horizontal (sometimes even vertical) privacy risks

Individual privacy

Critical privacy literacy

(1) Ability to identify, question, and critize societal structures, processes, norms and practices that affect individuals privacy on a societal level

(2) Development of social responsibility and motivation to take become agents of social change

Collective privacy

**Figure 1.** A comprehensive model of online privacy literacy.

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

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

### *2.3. Privacy and Data Protection Skills*

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

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

### *2.4. Critical Privacy Literacy*

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

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

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

## 3. Functions of Online Privacy Literacy

Based on the multidimensional model presented above, the role of online privacy literacy is twofold (cf. Figure 2). On the one hand, it empowers individuals (at least to some degree) to protect themselves against social, economic, and institutional influences. Online privacy literacy allows them to implemented data protection strategies and privacy regulation strategies by themselves (hereinafter called self-data protection) or by 'enforcing' data protection through laws and regulations (hereinafter called legal data protection). On the other hand, online privacy literacy—and in particular critical privacy literacy—can be regarded as a fundamental basis for the realization of citizens' democratic potential and, in turn, as a motivator of societal transformations. In the following, I will discuss both roles in more detail.

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

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

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

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

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

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

### *3.2. Motivating Individuals to Become Agents of Social Change*

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

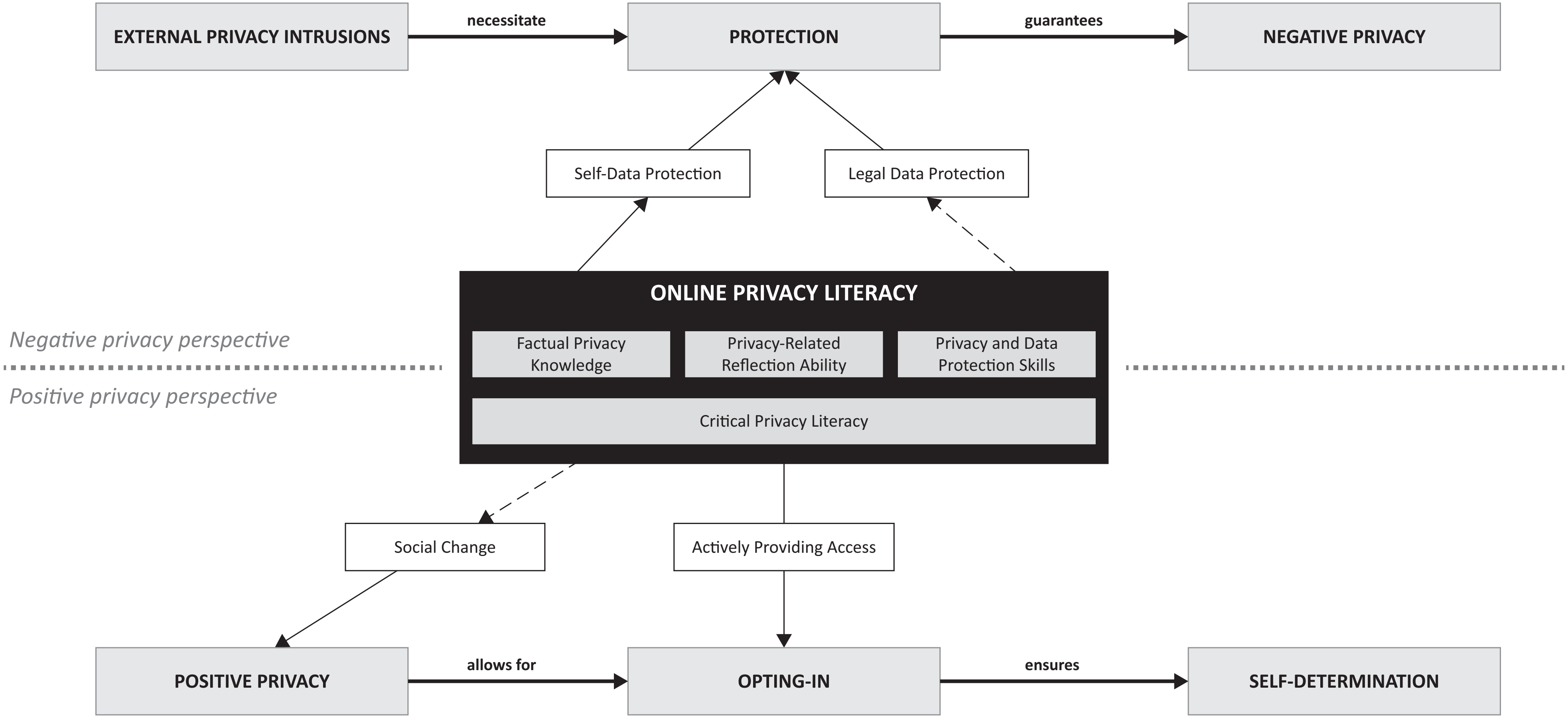

EXTERNAL PRIVACY INTRUSIONS
necessitate
PROTECTION
guarantees
NEGATIVE PRIVACY
Self-Data Protection
Legal Data Protection
ONLINE PRIVACY LITERACY
Factual Privacy Knowledge
Privacy-Related Reflection Ability
Privacy and Data Protection Skills
Critical Privacy Literacy
Negative privacy perspective
Positive privacy perspective
Social Change
Actively Providing Access
POSITIVE PRIVACY
allows for
OPTING-IN
ensures
SELF-DETERMINATION

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

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

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

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

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

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

## 4. Conclusion and Future Perspectives

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

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

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

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

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

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

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

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

## Conflict of Interests

The author declares no conflict of interests.

## References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

German Constitution. art 1, §1.

German Constitution. art. 2, §1.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the surveillance state*. New York, NY: Hamish Hamilton.

Groeben, N. (2002). Dimensionen der Medienkompetenz: Deskriptive und normative Aspekte [Dimensions of media literacy: Descriptive and normative aspects]. In N. Groeben & B. Hurrelmann (Eds.), *Medienkompetenz: Voraussetzungen, Dimensionen, Funktionen* [Media literacy: Requirements, dimensions, functions] (pp. 160–197). Weinheim: Juventa.

Gutwirth, S., Leenes, R., & de Hert, P. (Eds.). (2015). *Reforming European data protection law* (Vol. 20). Dordrecht: Springer.

Gutwirth, S., Leenes, R., & de Hert, P. (Eds.). (2016). *Data protection on the move: Current developments in ICT and privacy/data protection* (Vol. 24). Dordrecht: Springer.

Hobbes, T. (1651). *Leviathan*. Seattle, WA: Pacific Publishing Studio.

Hobbs, R., & Frost, R. (2011). Measuring the acquisition of media-literacy skills. *Reading Research Quarterly*, *38*(3), 330–355.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1589864

Horvát, E.-Á., Hanselmann, M., Hamprecht, F. A., & Zweig, K. A. (2012). One plus one makes three (for social networks). *PLoS ONE*, *7*(4). https://doi.org/10.1371/annotation/c2a07195-0843-4d98-a220-b1c5b77a7e1a

Jacobson, M., & Ruddy, M. (2004). *Open to outcome: A practical guide for facilitating and teaching experiential reflection*. Oklahoma City, OK: Wood N. Barnes.

Kellner, D., & Share, J. (2007). Critical media literacy, democracy, and the reconstruction of education. In D. Macedo & S. R. Steinberg (Eds.), *Media literacy: A reader* (pp. 3–23). New York, NY: Peter Lang.

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

Kolb, D. A. (2014). *Experiential Learning: Experience as the source of learning and development* (2nd ed.). Upper Saddle River, NJ: Pearson FT Press.

Kraus, L., Wechsung, I., & Möller, S. (2014). *A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior*. Paper presented at the Workshop on Privacy Personas and Segmentation (PPS) at the Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA, USA.

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, *7*(1), 3–14. https://doi.org/10.1080/10714420490280152

Martens, H., & Hobbs, R. (2015). How media literacy supports civic engagement in a digital age. *Atlantic Journal of Communication*, *23*(2), 120–137. https://doi.org/10.1080/15456870.2014.961636

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Masur, P. K. (2018a). Mehr als Bewusstsein für Privatheitsrisiken. Eine Rekonzeptualisierung der Online: Privatheitskompetenz als Kombination aus Wissen, Fähig und Fertigkeiten [More than risk awarness: A reconceptualization of online privacy literacy as a combination of knowledge, abilities, and skills]. *Medien & Kommunikationswissenschaft*, *66*(4), 446–465. https://doi.org/10.5771/1615-634X-2018-4-446

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

Masur, P. K., Teutsch, D., Dienlin, T., & Trepte, S. (2017). Online-Privatheitskompetenz und deren Bedeutung für demokratische Gesellschaften [Online privacy literacy and its role in democratic societies]. *Forschungsjournal Soziale Bewegungen*, *30*(2), 180–189.

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS) [Development and validation of the online privacy literacy scale (OPLIS)]. *Diagnostica*, *63*(4), 256–268. https://doi.org/10.1026/0012-1924/a000179

Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data." *Journal of Information, Communication and Ethics in Society*, *12*(2), 93–106. https://doi.org/10.1108/JICES-08-2013-0030

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection: Empowerment or burden? In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Data protection on the move* (pp. 277–305). Cham: Springer.

Mihailidis, P., & Thevenin, B. (2013). Media literacy as a core competency for engaged citizenship in participatory democracy. *American Behavioral Scientist*, *57*(11), 1611–1622. https://doi.org/10.1177/

0002764213489015

Mill, J. S. (2015). *On liberty*. Middleton: CreateSpace. (Original work published 1859)

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

Moore, B. (1984). *Privacy: Studies in social and cultural history*. New York, NY: Pantheon Books.

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford Law Books.

Ochs, C., & Lamla, J. (2017). Demokratische Privacy by Design [Democratic privacy by design]. *Forschungsjournal Soziale Bewegungen*, *30*(2), 189–199. https://doi.org/10.1515/fjsb-2017-0040

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

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

Potter, W. J. (2008). *Media literacy* (4th ed.). Los Angeles, CA: Sage.

Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, *4*(4), 323–333.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First *Monday*, *15*(1). https://doi.org/10.5210/fm.v15i1.2775

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online*, *64*, 88–92.

Sarigol, E., Garcia, D., & Schweitzer, F. (2014). Online privacy as a collective phenomenon. In A. Sala, A. Goel, & K. Gummadi (Eds.), *Proceedings of the Second ACM conference on online social networks* (pp. 95–106). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/2660460.2660470

Seubert, S., & Becker, C. (2019). The culture industry revisited: Sociophilosophical reflections on ‘privacy’ in the digital age. *Philosophy & Social Criticism*, *45*(8), 930–947. https://doi.org/10.1177/0191453719849719

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

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

Solove, D. J., & Schwartz, P. M. (2019). *Privacy law fundamentals.* Portsmouth, NH: International Association of Privacy Professionals.

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

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

The Economist Intelligence Unit. (2020). *Democracy index 2019: A year of democratic setbacks and popular protest*. London: The Economist Intelligence Unit.

TOR. (2020). The Onion Router. Retrieved from https://www.torproject.org

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

Trepte, S., & Masur, P. K. (2017). The need for privacy. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of personality and individual differences*. (pp. 1–4). London: Springer.

Trepte, S., & Reinecke, L. (2011). The social web as shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 61–74). Berlin: Springer.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Dordrecht: Springer.

Turow, J. (2003). *Americans online privacy: The system is broken* (Report 6-2003). Philadelphia, PA: The Annenberg Public Policy Center of the University of Pennsylvania.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Wolf, R. d., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, *35*, 444–454. https://doi.org/10.1016/j.chb.2014.03

Zuboff, S. (2019). *The age of surveillance capitalism*. New York, NY: Public Affairs.

## About the Author

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

**Media and Communication (ISSN: 2183–2439)**
**2020, Volume 8, Issue 2, Pages 270–279**
**DOI: 10.17645/mac.v8i2.2761**

Article

# Staying at the Edge of Privacy: Edge Computing and Impersonal Extraction

Luke Munn

Institute for Culture and Society, Western Sydney University, Penrith, NSW 2751, Australia;
E-Mail: l.munn@westernsydney.edu.au

Submitted: 5 January 2020 | Accepted: 12 May 2020 | Published: 23 June 2020

**Abstract**
From self-driving cars to smart city sensors, billions of devices will be connected to networks in the next few years. These devices will collect vast amounts of data which needs to be processed in real-time, overwhelming centralized cloud architectures. To address this need, the industry seeks to process data closer to the source, driving a major shift from the cloud to the 'edge.' This article critically investigates the privacy implications of edge computing. It outlines the abilities introduced by the edge by drawing on two recently published scenarios, an automated license plate reader and an ethnic facial detection model. Based on these affordances, three key questions arise: what kind of data will be collected, how will this data be processed at the edge, and how will this data be 'completed' in the cloud? As a site of intermediation between user and cloud, the edge allows data to be extracted from individuals, acted on in real-time, and then abstracted or sterilized, removing identifying information before being stored in conventional data centers. The article thus argues that edge affordances establish a fundamental new 'privacy condition' while sidestepping the safeguards associated with the 'privacy proper' of personal data use. Responding effectively to these challenges will mean rethinking person-based approaches to privacy at both regulatory and citizen-led levels.

**Keywords**
artificial intelligence; cloud; edge computing; personal data; privacy; smart city; surveillance

**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

Cloud architectures have reached a crisis point. From self-driving cars to smart city sensors; 30 billion devices will be connected to networks in the next few years (Stack, 2018). Yet existing cloud infrastructures are not designed for their needs. As Shi and Dustdar (2016, p. 78) explain; "the bandwidth of the networks that carry data to and from the cloud has not increased appreciably. Thus; with edge devices generating more data; the network is becoming cloud computing's bottleneck." Connected medical devices will generate huge volumes of data, connected cars will need near real-time processing, and connected cameras will capture extremely personal information. These three properties—data volume, data latency, and data privacy—are driving a shift away from the cloud model (Simonelli, 2019).

The technology industry aims to address these needs by moving computation and storage to where it is needed. Over the next few years; this will mean shifting many applications from centralized data center facilities to highly distributed devices at the edge of the network—from the center to the 'edge' or from the cloud to the 'fog.' Simply put, the edge is both a paradigm and an architecture that aims to store and process data closer to the source. Rather than having to move massive volumes of data all the way back to the cloud—a slow, expensive; or even unviable proposition—the edge processes it on site, addressing both latency and bandwidth issues. In doing so, the edge functions as a distributed layer of intelligence deployed at a local level (Luan et al., 2015). Practically this will take the form of cameras, sensors, switches, and micro-servers installed throughout vehicles, homes, workplaces, neighborhoods, and the broader urban environment. Following Shi and Dustdar (2016, p. 79) then, an edge device is "any computing or networking resource residing between data sources and cloud-based data centers." A smartphone could act as the edge between the body and the cloud; a smart home gateway could be the edge device between the home and the cloud.

In capturing, processing, and distributing highly personal information, the shift to the edge introduces critical new challenges to privacy. Yet existing scholarship on the edge and privacy is largely constrained to computer science and security, focusing tightly on solving specific technical problems (Alrawais, Alhothaily, Hu, & Cheng, 2017; Mukherjee et al., 2017; Roman, Lopez, & Mambo, 2018; Yi, Qin, & Li, 2015). Instead, this article poses a different research question: How are privacy-related conditions modulated by the edge, and what are the social and individual implications of this modulation? If the edge was always predicted to be a technical challenge, a 'non-trivial' extension to the cloud (Bonomi, Milito, Zhu, & Addepalli, 2012) it is also a highly political technology in transforming the way data can be handled and information extracted. The article will argue that the edge allows a form of individualization without identification, shaping privacy conditions while sidestepping the harder regulatory frameworks associated with 'personal data' as it is conventionally understood.

First, this article outlines the capabilities of the edge and introduces two specific understandings of privacy. Then, it posits two edge computing scenarios: ethnic facial recognition and an automated license plate reader. In each scenario, edge devices extract data and transform it into actionable insights, but then anonymize or abstract it before transferring it back to centralized data centers. The new affordances of the edge thus introduce new decisions around data. After that, the article poses these questions: what data to collect, how to process it at the edge, and how to 'complete' it in the cloud. Finally, the article discusses the implications of this shift, in establishing an intermediate layer of intelligence between the user and the cloud, edge computing circumvents some of the traditional privacy safeguards that have focused heavily on personal data collection and cloud storage.

## 2. Privacy Proper vs. Privacy Conditions

Much of the computer science literature surrounding privacy and the edge has focused on the security of personal data. While cloud data centers have developed a formidable array of hardware and software security features over time, edge-based hardware—consumer products like cameras, phones, and wearable devices—often only feature consumer-level protections. Such devices are often 'resource poor,' their micro-controllers were not designed for connectivity and lack the processing power to run cryptographic procedures, resulting in security issues such as authentication, access control, and data protection (Alrawais et al., 2017, p. 35). Moreover, rather than the closed ecosystem of the centralized data center, where a company can control access to servers, edge networks are a far more open, unrestricted architecture composed of potentially hundreds or thousands of devices, often operated by different providers. Because of this lack of a global perimeter, edge computing is more susceptible to rogue gateway attacks, where network nodes pretend to be legitimate and coax users to share data with them (Roman et al., 2018, p. 13). Edge hardware thus presents a highly vulnerable site, open to exploits. Stored on a diverse array of devices, many with minimal consumer-grade protections, this information presents a rich target for leaks and hacks. Already there have been a number of high-profile attacks exploiting these weaknesses. From cardiac devices at St Jude's Hospital to the TRENDnet webcam hack and the Mirai botnet that caused large sections of the Internet to go down, these examples demonstrate that "much of the embedded firmware running connected devices is insecure and highly vulnerable, leaving an indeterminate number of critical systems at risk" (Dunlap, 2017).

If edge hardware itself is more vulnerable, the content it captures only amplifies these concerns. Edge devices have significantly more potential to collect highly personal and highly detailed data. From health monitors to home assistants, many of these devices will be physically close to users or situated in the heart of their living environments, capturing more intimate data. The onboard camera of a self-driving car, for instance, will be switched on and recording for the entire duration of a driving session (Bloom, Tan, Ramjohn, & Bauer, 2017). It might be capturing the driver's face, but also her surrounding world, including her children and passengers. Edge-computing means this data no longer has to be heavily compressed snapshots that can be transferred to the cloud. From a privacy perspective, lifting this technical constraint means that a camera can be both higher resolution and lower latency, allowing the capture of a glance, for instance, at 60 frames per second. Moreover, devices on the edge, whether comprising a smartphone, a wearable device, a vehicle, or a network of cameras distributed throughout an urban space, have the potential to capture fine-grained location data. Locational data alone is highly valuable, aggregated over time it becomes a timeline of an individual's movements, providing an incisive window into their habits, behaviors, and preferences. As Barreneche and Wilken (2015) assert, such locational data becomes a sophisticated form of 'geodemographic profiling' that can then be leveraged for predictive purposes. Already we've seen how such locational data can be used to harass and target individuals, whether by law enforcement agencies (Munn, 2018) or private companies (Hill, 2014).

Overall, then, edge literature conflates privacy with personal data security. In this view, while the problem is technically challenging, it is theoretically straightforward—translating existing technologies like encryption to the edge will ensure 'privacy' for all (Zhang, Chen, Zhao, Cheng, & Hu, 2018; Zhang, Wang, Du, & Guizani, 2018).

In focusing on the security of personal data, edge literature coheres closely to the concept of privacy developed by the General Data Projection Regulation (GDPR), a version of privacy I will term 'privacy proper.' While the GDPR was conceived in the European Union, its definitions and framings have been taken up by various countries around the world. Applied to over 500 million citizens, the GDPR now forms one of the "de facto global standards for data privacy and protection" (Barrett, 2019). For the GDPR, personal data is key. "The term 'personal data' is the entryway" to the application of the regulation, states the law, "only if a processing of data concerns personal data" does the GDPR apply (European Commission, 2018). What exactly constitutes personal data? The regulation states that "data must therefore be assignable to identified or identifiable living persons to be considered personal" (European Commission, 2018). Once data conforms to this definition, the company or agency becomes a 'data processor' who must maintain compliance—hamstrung in terms of what kinds of data may be captured, how it may be stored and accessed, and which borders it may cross. In this article, privacy proper will thus designate a threshold that actors do not wish to cross, a regulatory minefield triggered when organizations begin dealing with personal data.

Certainly, the edge presents some obvious challenges for personal data security. Yet more subtly, the edge may shape privacy-related abilities without necessarily processing or storing personal data. To differentiate this possibility, I introduce a second term, 'privacy condition,' drawing on recent work by legal scholar Julie Cohen. To rescue privacy from vague rhetoric and unenforceable ideals, Cohen begins not from the figure of the self, but from the ground of the underlying conditions "that are needed to produce sufficiently private and privacy-valuing subjects" (Cohen, 2019, p. 1). If rights discourse and legal rhetoric can be abstract, then conditions have a specificity, a concreteness. Conditions actively enable some privacy-related abilities while making others improbable or even impossible. Digital data and the sharing of information has made the stakes of these abilities and inabilities suddenly very clear. This is why, even though privacy clearly has a long lineage in liberal political philosophy, Cohen stresses that privacy is a "paradigmatic information-era right," one not defined by rights discourse, but by the conditions established within the "political economy of informationalism" (Cohen, 2019, p. 2; see also Cohen, 2017).

Given this framing, Cohen wants to focus on the particular set of "design, production, and operational practices' most likely to produce privacy-valuing conditions" (Cohen, 2019, p. 1). A distinct version of privacy emerges from a set of affordances, the possible range of uses made available by an object or environment (Cohen, 2019, p. 12). In other words, particular privacy conditions emerge from particular technical configurations. As a nascent technology, the edge enables new affordances, allowing subjects to be apprehended, mediated, and responded to in distinct new ways—even when, or especially when, so-called personal data is never handled. With these two terms defined, the following scenarios focus on how edge affordances modulate privacy conditions while allowing actors to sidestep the requirements attached to privacy proper.

## 3. Two Scenarios

The first scenario is license plate capture and analysis, drawn from a recent article on hybrid cloud-edge computing (Zhang, Zhang, Shi, & Zhong, 2018). The authors lament the siloed nature of current data collection. They suggest that many public and private agencies would have an interest in obtaining license plate data in order to understand where citizens are located and where they travel to. Yet due to anxieties around data sharing and user authentication, each of these institutions conducts their own data capture and maintains their own cloud-based repository. The result is that "data owned by multiple stakeholders is rarely shared among data owners" (Zhang et al., 2018, p. 2004).

The edge introduces new possibilities into this scenario. For one, edge nodes can act as a nexus, combining data sources from multiple stakeholders. As Zhang et al. (2018, p. 2005) suggest, footage from the on-body cameras of police officers could be combined with squad car camera feeds, mobile uploads and more traditional CCTV feeds to form a far more extensive and comprehensive data source. Data can be assembled from various sources, processed in order to remove sensitive information, and then distributed to stakeholders. The edge's ability to decouple data collection from data storage thus has the potential to foster formerly unworkable alliances. For instance, Zhang et al. (2018, p. 2005) note that both private insurance companies and public district health boards would be interested in some of the same data. Groups of institutions might band together to collect license plate data, smart city data, or health data, creating broad infrastructures of surveillance.

Of course, this indiscriminate surveillance introduces a range of problems if privacy proper is invoked. Any one of these raw video feeds might capture facial details that could be used to identify an individual, overstepping the privacy boundaries allowed by an institution. Yet the edge can again provide a solution. In aggregating this data at a site long before it arrives back at the cloud, the edge acts as a kind of pre-processor for data. Rather than transferring all of the raw video data back to the cloud, Zhang et al. (2018, p. 2005) propose that the edge node conducts video clipping, scanning "video streams to selectively filter out frames with a license plate." Edge computation would locate only those frames where black letters on a white background indicate a license plate. Each frame is then cropped to only show the plate, and optical character recognition technology converts the plate photograph to its alphanumeric equivalent, e.g., CLA974. Finally, this small text field is transferred to the cloud facilities of each stakeholder. By introducing an intermediary layer between capture and cloud, between user and stakeholder, the edge also introduces a new set of privacy-challenging affordances. Data can be collected from multiple stakeholders but then parsed at the edge, selected, sampled, and scrubbed before continuing on to cloud-based facilities. These dynamics can also be seen in the next scenario of edge computing.

The second scenario is the facial detection of ethnic minorities. In 2019, Wang, Zhang, Liu, Liu, and Miao published the article 'Facial Feature Discovery for Ethnicity Recognition.' While this article was not explicitly posited as an edge application, speculating about its transfer to this domain is hardly a leap. Indeed, as a slew of recent technical articles suggest, researchers are already embracing the new possibilities that edge computing offers for facial detection in urban areas (Dautov et al., 2018), crowd monitoring (Bailas, Marsden, Zhang, O'Connor, & Little, 2018), and intelligent surveillance (Hu et al., 2018), with one going so far as to call real-time video analytics the edge's 'killer app' (Ananthanarayanan et al., 2017).

Wang, Zhang, and Taleb (2018, p. 1) begin by noting that "the analysis of race, nation, and ethnical groups based on facial images is a popular topic recently in face recognition community." Bypassing even the barest consideration of ethics, the authors suggest that this new field would naturally be beneficial for state actors wishing to enforce certain restrictions on their citizens: "With rapid advance of people globalization…face recognition has great application potential in border control, customs check, and public security" (Wang et al., 2018, p. 1) The disturbing enthusiasm for such privacy-impinging surveillance is not limited to China, but is increasingly evident across cities in Ecuador, Pakistan, Kenya, Germany, and the United Arab Emirates (Mozur, Kessel, & Chan, 2019).

Yet, frustratingly for the article's authors, ethnicity can often be difficult to detect, either because the morphologies of race are too subtle or because the individual contains traces of multiple ethnicities. The problem, from an engineering perspective, is that "the gene of one ethnical group is hardly unique and it may include various gene fragments from some other ethnical groups" (Wang et al., 2018). Fortunately, facial aspects can be analyzed in a far more fine-grained manner through computational technologies in order to reveal their ethnicities. The authors set about identifying three ethnic groups: Uighur, Tibetan, and Korean (Wang et al., 2018). The article, like many in machine learning, essentially lays out the steps used to produce the model and measures its effectiveness against competing models. The model is trained on an image set of university students, and gradually learns to identify the three ethnic groups with more success, displaying progressively lower levels of uncertainty.

Key for the authors' model is the extraction of a 'T' feature from the center of each photograph containing the lips and nose (Wang et al., 2018). While the T varies with each ethnic group, these morphological features are considered to be the telltale markings that distinguish whether an individual is within the targeted ethnic group. Indeed, the extraction of the T, while obviously deleting key facial information, amplifies the model's ability to detect ethnicity. As the authors note that "actually, the facial features extracted from the 'T' regions are more suitable for ethnicity recognition since the unrelated information has been filtered out" (Wang et al., 2018). In this application, the full photograph of the individual is unnecessary or even a distraction. The model does not need to do the computationally intensive work of facial identification—who exactly an individual is—but rather the simpler task of determining whether an individual is 'ethnic' or not.

Such a technology would seem tailor made for the edge. As more cameras are connected to networks, the possibilities of surveillance grow. However, video data itself is massive, becoming both economically expensive and technically infeasible if it is sent back to the cloud. As the authors of one study suggested, processing raw video from widely distributed "CCTV cameras and mobile cameras not only incurs uncertainty in data transfer and timing but also poses significant overhead and delay to the communication networks" (Nikouei et al., 2018, p. 1). In the cloud model, images need to be sent from all the cameras to a data center facility via the network, be processed in this centralized facility, and then the result delivered to a client or end-user. This lengthy process not only introduces significant latency, but makes some surveillance applications essentially unviable from a technical perspective.

Instead, the edge allows processing to be conducted at the source. No identifying image needs to be sent back to the cloud and compared against an exhaustive database of citizens. No personal data is 'collected' by the agency in the sense of being transmitted to a data center where it will be held indefinitely in a database or stored on a hard disk. Instead, this machine-learned model could be compressed and loaded onto a small edge-based device with a camera. Such a device would then process its image feed in real-time, rapidly determining whether an individual is 'ethnic' or not.

Once determined, this compressed yet highly consequential piece of information might be used in any number of ways. In border security, for instance, one could imagine a green light turning red and a passenger selected for additional screening. In a smart city scenario, this data might be paired with a camera's location and uploaded to form an aggregated portrait of ethnic populations over time. Such data is based on an individual but rendered impersonal, providing insights for governance while sidestepping the harder restrictions around personal data. From a broader political perspective, the scenario demonstrates how edge affordances might underpin new forms of less governed control, establishing a privacy condition that avoids directly confronting the regulatory apparatus attached to privacy proper.

## 4. Questions for Privacy at the Edge

The edge complicates established privacy conditions, reopening critical debates about the ways such informational architectures may impact the everyday lives of individuals and amplify existing power asymmetries. While the scenarios above raised some of these issues indirectly, in the next sections they form three explicit questions.

### *4.1. What Data Will Be Collected at the Edge?*

As millions of new devices are connected to networks over the next few years, the possibilities of data capture will also proliferate. As discussed, these devices, located in the home, on the wrist, or stationed around the neighborhood, will be able to capture fine-grained, highly personal data. While some network constraints will certainly still persist, edge computing means that data collection practices are no longer dictated so tightly by transmission back to the cloud. Indeed, as mentioned above, it is precisely these possibilities that have led to the many articles on real-time monitoring, crowd monitoring and ‘intelligent surveillance’ via edge computing (Ananthanarayanan et al., 2017; Bailas et al., 2018; Dautov et al., 2018; Hu et al., 2018). This literature displays a general rush to embrace these possibilities, even though these applications have clear implications for privacy intrusions and personal freedoms. What these enthusiastic responses demonstrate is that in many ways it was technics, rather than ethics, which limited the extent of previous intrusions into personal data. Network speeds, bandwidth capacities and physical distance were hard restrictions. To a significant degree, edge computing lifts these constraints, providing more freedom to public and private actors wishing to delve further into individuals and their lives.

These capabilities mean that the question of data collection will hinge less on technical and economic concerns (cost to transfer gigabytes back to the cloud) and more on company culture, ethical values, and policy stipulations—if these are even in place. With technical constraints lifted, companies will be under increased pressure to collect more, and more intrusive data, which could provide key business insights. Yet individual companies are not entirely free in navigating this ethical terrain. Companies do not operate in isolation, but within competitive industries, particularly the highly contested technology field. Given these conditions, companies are subject to the “coercion of competition” (Marx, 2004, p. 675). If one company chooses not to push the ethical boundaries of data capture, others will (Kokalitcheva, 2019). At a time when comprehensive data has become highly valuable, this decision grants one company strategic advantage over their competitors.

### *4.2. How Will Data Be Processed at the Edge?*

The edge introduces an additional layer of mediation between users and the cloud, forming a site for processing data after it has been captured, but before it is stored and centralized. As suggested by the scenarios above, this interposition creates new possibilities for data processing. Rich, highly detailed data can be captured by edge devices and then processed by an edge hub in order to extract nuggets of valuable information, which is then passed back to a centralized cloud facility.

Abstraction becomes a key term within this process. How will highly personal data be transformed into impersonal, anonymized data? Here edge computing can draw on a number of existing technologies, from k-anonymity (Sweeney, 2002) to micro-aggregation (Domingo-Ferrer, Sánchez, & Soria-Comas, 2016). These established techniques, broadly applicable to any information set, include substitution, in which identifying values are randomly replaced, shuffling, so that associations between variables are lost, sampling, in which a partial set from the whole is transmitted, and variance, in which numerical values are perturbed or altered (Curzon, Almehmadi, & El-Khatib, 2019). Certainly, such technologies provide established means of handling particular types of data and aspects of applications. Yet they can also become a way of black-boxing problems and arriving too quickly at a ‘privacy solution.’

Instead, the task is to keep the question of data extraction in the foreground: How is data mediated at the edge and what is lost or gained in this intermediation? Highly specific location data, for instance, might be captured at the edge, but then generalized into a district or combined with other user locations. A gender field might be used in an edge calculation, but then dropped, something users may or may not want. An individual’s race might be clumped into a parent category, imposing a statistical system and erasing specific origins. In every permutation, a slightly different data subject is rendered (see Cheney-Lippold, 2018; Koopman, 2019). These examples stress that the technical transformation of information also has political and social implications. Abstraction, then, should be seen less as a solution and more as a set of design decisions around data. These decisions come together to form a particular configuration of practices and protocols, establishing a privacy condition that imposes itself on subjects in certain ways.

For those tasked with making these design decisions, abstraction attempts to walk a tightrope, balancing the desire of states and corporations to “capture it all” against the desire of individuals and their “right to be let alone” (Warren & Brandeis, 1890, p. 193). To claim that nothing should ever be captured would be naïve, to claim that everything should would be unethical: “There is a natural tension between the quality of data and the techniques that provide anonymity protection,” observes Latanya Sweeney (2001, p. 33); given these tensions, the goal is to design an optimal release so that “the data remain practically useful yet rendered minimally invasive to privacy.” For both public and private actors, capturing valuable data while remaining sensitive to privacy issues will take care and consideration.

### *4.3. How Is Data Completed in the Cloud?*

If the edge is a site of intermediation, the cloud becomes the site of completion, where data is assembled together, integrated into more formal structures, and processed for additional insights. Completion stresses the aim of both public governments and private corporations to exhaustively analyze data. If data is capital, then in order to accrue more value, one must extract more data from more subjects, accumulate it in increasingly larger volumes, and mine it incessantly for insights (Sadowski, 2019). Here the resource-constrained environment of the edge leans heavily on the resource-rich environment of the cloud. Indeed, new data center architectures embrace this role as a site of intensive processing, developing dedicated chips with liquid cooling in order to support the heavy computation required by machine learning applications (Sverdlik, 2018). If these conditions are highly technical, the insights they derive from high intensity processing shapes privacy conditions in concrete ways.

Completion foregrounds the design of a data pipeline. Decisions made about (1) what data to capture and (2) how the edge processes that data must also take into account (3) how the cloud processes that data to arrive at productive insights. Here the cloud and the edge might supplement each other with their respective strengths and weaknesses. The edge is decentralized, with low latency but low power, capable of capturing much but processing, storing, and transmitting little. The cloud is centralized, ill-suited for capture with its high latency but excellent at processing and storage. Given these trade-offs, the edge needs to deliver low volume but high potential data that can be intensively processed by the cloud to generate value.

As the two scenarios discussed above suggested, a circuit for completing data and maximizing its value is already emerging. First, data is collected from devices distributed at the edge. This data is then distributed to the closest edge node, processed in order to clean up or sample the data, and then passed onto a centralized cloud facility, where it is assembled into a training set of machine learning. High intensity processing in the cloud is used to train a model based on this dataset, gradually becoming better over time. Once completed, the machine learning model is then compressed into a light-weight version and distributed back out to edge devices, where it can function autonomously.

Here we see a feedback loop, where captured information becomes training data, which in turn contributes to more comprehensive mechanisms of capture. Indeed, whole companies have emerged based on riding this loop of “embedding edge intelligence as close to the source of streaming sensor data as possible” (Foghorn Systems, 2019). If the realization of this approach is still nascent, it is clear that developing such machinic intelligence will follow the blueprint already laid down by broader regimes of technical capture and data analysis. The imperative is to more fully apprehend the individual and her lifeworld, to more exhaustively grasp her properties, her practices, and her sociocultural milieu (Harcourt, 2015; Pasquinelli, 2015; Steyerl, 2016). This circuit thus strives to delve ever further into the subject and her everyday life, gradually apprehending her bodily characteristics, daily behaviors, location over time, and social affiliations (Finn, Wright, & Friedewald, 2013), until no secrets remain.

While a company may complete its own data, completion might also be undertaken in a more unauthorized or unexpected way by others. Data collected at the edge might well be anonymised in a robust way before transmission to cloud storage facilities. However, as scholars have shown, data can be de-anonymised by integrating multiple datasets together and then cross-indexing values against each other (Narayanan & Shmatikov, 2008; Sweeney, 1997). Promises of unassailable privacy are often broken promises (Ohm, 2010). If the edge introduces a new set of decisions about how data will be appropriately handled and transformed, these scenarios warn companies and organizations that they must also take into account the combinatorial possibilities of the cloud as well.

## 5. End Run Around Privacy Protections

If edge computing holds out enticing promises, its abilities may also impinge on the freedoms of individuals and the rights of communities. In this sense, edge computing forms the latest incarnation of what Shoshana Zuboff (2019) has described as surveillance capitalism. For Zuboff (2015, p. 83), surveillance capitalism accumulates “not only surveillance assets and capital, but also rights” through “processes that operate outside the auspices of legitimate democratic mechanism.” Yet counter to Zuboff, rather than acquiring rights, these technical processes seek to never invoke rights. If big data accomplishes an “end run around procedural privacy protections” (Barocas & Nissenbaum, 2014, p. 31), then edge computing also carries out an ‘end run’ of its own. The goal is to extract data, value, and capital while never venturing into the legal and ethical minefield of privacy proper.

One way of doing this is to respond to the individual while filtering out, deleting, or abstracting away data deemed to be personal. The small, hyperlocal devices of the edge, situated in a smart home or a smart city, will be far more adept at latching onto the behaviors and bodies of individuals. The edge can respond to these inputs in the moment, without storing the names and identifiers typically associated with 'personal data.' As a site of preprocessing, the edge is able to draw upon single bodies and personal lives, yet immediately abstract this data or aggregate it into a depersonalized mass. In this sense, the edge resonates with Antoinette Rouvroy's observation that algorithmic governance strives to never confront the person in her entirety, to never directly call her up as a political subject. 'The only subject' such governmentality needs, Rouvroy (2013, p. 154) stresses, is a "unique, supra-individual, constantly reconfigurated 'statistical body' made of the infra-individual digital traces of impersonal, disparate, heterogeneous, dividualized facets of daily life and interactions." A subject is apprehended at an individual level, but not necessarily identified.

Indeed, running through all these edge scenarios is the sense that the former key question—whether or not a user can be identified—may be subsumed by a far more fundamental question: What forms of life are being extracted from the user *even though* they are not identified? The de facto framing of privacy proper ushered in by the GDPR has privileged personal data. Yet this entire legal edifice of protections only applies once this definition is reached. Perhaps data never needed to be personal to be valuable. Perhaps control may be enacted and maintained without identifying a unique individual. Indeed, recent work on group privacy (Floridi, 2014; Mittelstadt, 2017; Taylor, Floridi, & Van der Sloot, 2016) responds precisely to this realization. Even without explicit identification, the new spaces enabled by edge computing present a verdant territory for extractive regimes (Mezzadra & Neilson, 2019), a rich zone of markers and moments to capture and respond to. While this extractivist logic deals with each person in turn—capturing moods and faces, responding to bodies and individual inputs, identifying movements and work performances—its value is only obtained by aggregating this data, by assembling and mining it en masse. This is why Tiziana Terranova (2018, p. 1) stresses that the "extractivism of data capital" siphons off the energetic behaviors and activities of the broader social body. The edge suggests a form of extraction that is individualized but not personalized.

If the individual-but-impersonal is one way of carrying out an end run around privacy, then another is avoiding some of the sharper points of personal data laws. While several existing laws regulate data that is 'held' (Mexican Congress, 2010) or 'stored' (U.S. Congress, 2018), the edge provides a new intermediary layer of intelligence where data can be captured, derived from, and then discarded or fundamentally transformed before it is stored. Through this affordance, the edge establishes a new frontier site for processing, a grey zone that seems sparsely covered by existing legislation, which has so far focused heavily on a centralized cloud model. The technology industry is all-too-aware of this possibility, even if it is framed as law abiding. "To avoid breaking the new law and thus being fined, companies should keep most of the data collected out of the cloud and process it at the edge" recommends one tech pundit (Valerio, 2018). Far more effective than eroding privacy is never confronting privacy proper to begin with.

How might we respond to the new privacy conditions instantiated by edge architectures? Regulators and policymakers will need to develop a broader and more nuanced understanding of the cloud. If centralized, hyperscale data centers remain at the core of cloud computation, the edge connects a cascading set of devices from regional hubs all the way down to local base stations and wearable and personal devices. These devices, though low-powered and often overlooked, form the new frontier for data collection practices, passing information streams up the chain, where it is aggregated together before finally arriving at the traditional data center. Yet if this ecosystem is vast, it is not monolithic. Devices at each level have distinct capacities. For example, the heavy encryption assumed in a full-scale data center may be impossible on many low-end edge devices. Regulation will thus need to be expansive but also articulated, developing codes and guidelines appropriate for each level of this architecture.

Along with acknowledging the new constellation of architectures that comprise the cloud, regulation also needs to address the edge's more situated, responsive capabilities. As the scenarios above suggested, the concept of storing an individual's personal information in a centralized database comes at the end of a long chain of activities and possibilities—or never at all. While edge devices certainly function as key points of capture, they will also carry out important processing operations, especially as hardware and software within this nascent field matures. Machine learning models, as discussed, are already being embedded in edge devices, meaning that facial detection, video trimming, and other key operations can take place within the device itself in real-time. Such data may be retained, abstracted into less 'personal' forms and transmitted back to the cloud—or simply discarded to make way for the next interaction. In doing so, edge-based devices will allow individualized interactions in the moment without having to fully confront the person and her associated rights. These technical abilities thus require a political and epistemological shift in privacy safeguards. Rather than beginning from the autonomous individual and her bundle of rights, rethinking privacy conditions from an operational standpoint as Cohen did might prove more suited for our era of rapid technological change.

For their part, citizens, activists, and organizations might productively question this model of personal privacy. Instead of this person-based approach, they might move to more communal models, based on the group, the neighborhood, the city, or the broader community. Evgeny Morozov (2015, 2018a, 2018b) has been at the forefront of this questioning, long arguing that the current model provides nominal protection for the individual, while continuing to funnel valuable data to tech giants—Google, Amazon, Facebook, and others—who monetize it for financial gain. Instead, he suggests a socialized infrastructure where citizens could pool together their data. This public data commons can be leveraged by technologies for the public good, directing value back into the hands of the data producers. This approach recognizes that individuals have little purchase on a political economy predicated on de-individualized, aggregated data. Instead, thinkers like Morozov and other data commons advocates (Jarman & Luna-Reyes, 2016; Shkabatur, 2018; Simon, 2018) join group privacy theorists (Mittelstadt, 2017; Taylor et al., 2016) in recognizing that privacy demands are both politically amplified and technically clarified when coming from a community. What would this community-based understanding of privacy look like on an everyday operational level? Due to the edge's emergent nature, more work is needed to bring together the technical, social, and legal and develop a workable privacy model attentive to the novel conditions that the edge introduces.

## 6. Conclusion

This article has explored how the shift to edge computing introduces new privacy challenges. While widely covered in engineering and computer science research, there have been few, if any, studies on the cultural, social, and political implications of edge computing. Given this gap, this article has merely introduced some key concepts and sketched out some initial possibilities. More research is urgently needed to examine the tensions and decisions ushered in by this paradigm, moving beyond technical capabilities to focus on social and ethical responsibilities. After defining the edge and two framings of privacy, the article posited two scenarios drawn from real-world engineering articles: an ethnic facial detection model and an automated license plate reader. While personal data security has been the traditional focus, these scenarios suggested that the edge poses a more subtle and significant set of questions. The technical affordances of the edge allow data to be captured, processed, and completed in new ways. Such decisions establish a significant privacy condition, shaping the ways in which consumers are targeted and the methods by which subjects are governed. They suggest that asymmetric power relations might be amplified while avoiding existing privacy regulation, slipping through the definitions of personal data established by current data safeguards. In this sense, novel network architectures open up a legal and ethical loophole. If the edge is seen as a technical solution, it also presents a political solution, facilitating a mode of power able to target the individual without crossing the threshold of privacy proper.

## Acknowledgments

This research work was supported as part of the wider project 'Data Centres and the Governance of Labour and Territory,' an Australian Research Council Discovery Project (DP160103307).

## Conflict of Interests

The author declares no conflict of interests.

## References

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34–42.

Ananthanarayanan, G., Bahl, P., Bodík, P., Chintalapudi, K., Philipose, M., Ravindranath, L., & Sinha, S. (2017). Real-time video analytics: The killer app for edge computing. *Computer*, *50*(10), 58–67.

Bailas, C., Marsden, M., Zhang, D., O'Connor, N. E., & Little, S. (2018). Performance of video processing at the edge for crowd-monitoring applications. In H. Mueller, Y. Rongshan, & A. Skarmeta (Eds.), *2018 IEEE 4th world forum on Internet of Things (WF-IoT)* (pp. 482–487). Washington, DC: IEEE Computer Society.

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM*, *57*(11), 31–33.

Barreneche, C., & Wilken, R. (2015). Platform specificity and the politics of location data extraction. *European Journal of Cultural Studies*, *18*(4/5), 497–513.

Barrett, C. (2019). Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? *Scitech Lawyer, Chicago*, *15*(3), 24–29.

Bloom, C., Tan, J., Ramjohn, J., & Bauer, L. (2017). *Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles*. Paper presented at the 13th Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In M. Gerla & D. Huang (Eds.), *Proceedings of the first edition of the MCC workshop on Mobile cloud computing: MCC '12* (pp. 13–16). New Yor, NY: ACM Press.

Cheney-Lippold, J. (2018). *We are data: Algorithms and the making of our digital selves*. New York, NY: NYU Press.

Cohen, J. E. (2017). Affording fundamental rights: A provocation inspired by Mireille Hildebrandt. *Critical Analysis of Law*, *4*(1), 78-90.

Cohen, J. E. (2019). Turning privacy inside out. *Theoretical Inquiries in Law*, *20*(1), 1–32.

Curzon, J., Almehmadi, A., & El-Khatib, K. (2019). A survey of privacy enhancing technologies for smart cities. *Pervasive and Mobile Computing*, *55*, 76–95.

Dautov, R., Distefano, S., Bruneo, D., Longo, F., Merlino, G., Puliafito, A., & Buyya, R. (2018). Metropolitan intelligent surveillance systems for urban areas by harnessing IoT and edge computing paradigms. *Software: Practice and experience*, *48*(8), 1475–1492.

Domingo-Ferrer, J., Sánchez, D., & Soria-Comas, J. (2016). Database anonymization: Privacy models, data utility, and microaggregation-based inter-model connections. *Synthesis Lectures on Information Security, Privacy, & Trust*, *8*(1), 1–136.

Dunlap, T. (2017, May 10). The 5 worst examples of IoT hacking and vulnerabilities in recorded history. *IoT For All*. Retrieved from https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities

European Commission. (2018). *General Data Protection Regulation* (2016/679). Brussels: European Commission.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In S. Gutwirth, R. Leenes, P. de Hert, & Y. Poullet (Eds.), *European data protection: Coming of age* (pp. 3–32). Dordrecht: Springer. https://doi.org/10.1007/978-94-007-5170-5_1

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology*, *27*(1), 1–3.

FogHorn Systems. (2019, July 1). FogHorn Lightning. *FogHorn Systems*. Retrieved from https://www.foghorn.io/lightning-iot-edge-computing

Harcourt, B. (2015). *Exposed: Desire and disobedience in the digital age*. Cambridge, MA: Harvard University Press.

Hill, K. (2014, October 3). "God view": Uber allegedly stalked users for party-goers' viewing pleasure (updated). *Forbes*. Retrieved from https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure

Hu, H., Shan, H., Zheng, Z., Huang, Z., Cai, C., Wang, C., . . . Quek, T. Q. S. (2018). Intelligent video surveillance based on mobile edge networks. In S. Li (Ed.), *2018 IEEE international conference on communication systems (ICCS)* (pp. 286–291). New York, NY: IEEE. https://doi.org/10.1109/ICCS.2018.8689194

Jarman, H., & Luna-Reyes, L. F. (2016). *Private data and public value: Governance, green consumption, and sustainable supply chains*. New York, NY: Springer.

Kokalitcheva, K. (2019, July 2). A wave of tech companies have pushed ethical boundaries to maximize profit. *Axios*. Retrieved from https://www.axios.com/big-tech-companies-ethics-facebook-doordash-59abf670-078d-4e15-9033-c0e6e6d75127.html

Koopman, C. (2019). *How we became our data: A genealogy of the informational person*. Chicago, IL: University of Chicago Press.

Luan, T. H., Gao, L., Li, Z., Xiang, Y., Wei, G., & Sun, L. (2015). Fog computing: Focusing on mobile users at the edge. *Cornell University.* Retrieved from http://arxiv.org/abs/1502.01815

Marx, K. (2004). *Capital: A critique of political economy* (B. Fowkes, Transl.). London: Penguin Books.

Mexican Congress. (2010). *Federal law on protection of personal data held by individuals* (DOF 05-07-2010). Mexico City: Mexican Congress.

Mezzadra, S., & Neilson, B. (2019). *The politics of operations: Excavating contemporary capitalism*. Durham, NC: Duke University Press.

Mittelstadt, B. (2017). From individual to group privacy in big data analytics. *Philosophy & Technology*, *30*(4), 475–494.

Morozov, E. (2015). Socialize the data centres! *New Left Review*, *91*(1), 45–66.

Morozov, E. (2018a, January). *DECODE presents: Data commons and the city* [Video file]. Retrieved from https://www.youtube.com/watch?v=Dfjx7W1jKO8

Morozov, E. (2018b, March 31). After the Facebook scandal it's time to base the digital economy on public v private ownership of data. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/mar/31/big-data-lie-exposed-simply-blaming-facebook-wont-fix-reclaim-private-information

Mozur, P., Kessel, J. M., & Chan, M. (2019, April 24). Made in China, exported to the world: The surveillance state. *The New York Times*. Retrieved from https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges. *IEEE Access*, *5*, 19293–19304. https://doi.org/10.1109/ACCESS.2017.2749422

Munn, L. (2018). Seeing with software. *Studies in Control Societies*, *2*(1). Retrieved from https://studiesincontrolsocieties.org/seeing-with-software

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In Y. Guan (Ed.), *IEEE symposium on security and privacy* (pp. 111–125). New York, NY: IEEE.

Nikouei, S. Y., Chen, Y., Song, S., Xu, R., Choi, B.-Y., & Faughnan, T. R. (2018). Smart surveillance as an edge network service: From harr-cascade, SVM to a lightweight CNN. *Cornell University*. Retrieved from http://arxiv.org/abs/1805.00331

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, *57*, 1701–1777.

Pasquinelli, M. (2015). Italian operaismo and the information machine. *Theory, Culture & Society*, *32*(3), 49–68.

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, 680–698.

Rouvroy, A. (2013). The end(s) of critique: Data behaviourism versus due process. In M. Hildebrandt & K. De Vries (Eds.), *Privacy, due process and the computational turn* (pp. 143–167). Abingdon: Routledge.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, *6*(1). https://doi.org/10.1177/2053951718820549

Shi, W., & Dustdar, S. (2016). The promise of edge computing. *Computer*, *49*(5), 78–81.

Shkabatur, J. (2018). *The global commons of data* (SSRN Scholarly Paper No. ID 3263466). Rochester, NY: Social Science Research Network.

Simon, D. (2018, November 27). Decentralized digital infrastructure: Towards digital commons. *Dezentrum*. Retrieved from https://www.dezentrum.ch/en/blog/decentralized-digital-infrastructure-towards-digital-commons

Simonelli, J. (2019, April 30). *DCD New York 2019 Q&A with Jim Simonelli, Schneider Electric* [Video file]. Retrieved from https://www.youtube.com/watch?v=m8iumNZycJU

Stack, T. (2018, February 5). Internet of Things (IoT) data continues to explode exponentially: Who is using that data and how? *CISCO*. Retrieved from https://blogs.cisco.com/datacenter/internet-of-things-iot-data-continues-to-explode-exponentially-who-is-using-that-data-and-how

Steyerl, H. (2016). A sea of data: Apophenia and pattern (mis-)recognition. *E-Flux*. Retrieved from https://www.e-flux.com/journal/72/60480/a-sea-of-data-apophenia-and-pattern-mis-recognition

Sverdlik, Y. (2018, July 31). When air no longer cuts it: Inside Google's AI-driven shift to liquid cooling. *Data Center Knowledge*. Retrieved from https://www.datacenterknowledge.com/google-alphabet/when-air-no-longer-cuts-it-inside-google-s-ai-driven-shift-liquid-cooling

Sweeney, L. (1997). Weaving technology and policy together to maintain confidentiality. *The Journal of Law, Medicine & Ethics*, *25*(2/3), 98–110.

Sweeney, L. (2001). *Computational disclosure control: A primer on data privacy protection* (Doctoral dissertation). Massachusetts Institute of Technology, Cambridge, MA.

Sweeney, L. (2002). K-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5), 557–570.

Taylor, L., Floridi, L., & Van der Sloot, B. (2016). *Group privacy: New challenges of data technologies* (Vol. 126). Cham: Springer.

Terranova, T. (2018). *Data mining the body of the socius*. Berlin: Staatliche Museen Zu Berlin. Retrieved from https://smart.smb.museum/export/downloadPM.php?id=5349

U.S. Congress. (2018). *CLOUD Act* (H.R. 4943). Washington, DC: U.S. Congress.

Valerio, P. (2018, October 31). To comply with GDPR, most data should remain at the edge. *IoT Times*. Retrieved from https://iot.eetimes.com/to-comply-with-gdpr-most-data-should-remain-at-the-edge

Wang, C., Zhang, Q., Liu, W., Liu, Y., & Miao, L. (2019). Facial feature discovery for ethnicity recognition. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(1), 1–17.

Wang, H., Zhang, Z., & Taleb, T. (2018). Editorial: Special issue on security and privacy of IoT. *World Wide Web*, *21*(1), 1–6.

Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Yi, S., Qin, Z., & Li, Q. (2015). Security and privacy issues of fog computing: A survey. In K. Xu & H. Zhu (Eds.), *International conference on wireless algorithms, systems, and applications* (pp. 685–695). New York, NY: Springer.

Zhang, H., Wang, Y., Du, X., & Guizani, M. (2018). Preserving location privacy in mobile edge computing. In X. You & C.-M. Chen (Eds.), *IEEE international conference on communications* (pp. 1–6). New York, NY: IEEE.

Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access*, *6*, 18209–18237.

Zhang, Q., Zhang, Q., Shi, W., & Zhong, H. (2018). Firework: Data Processing and Sharing for Hybrid Cloud-Edge Analytics. *IEEE Transactions on Parallel and Distributed Systems*, *29*(9), 2004–2017.

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

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: PublicAffairs.

## About the Author

**Luke Munn** uses both practice-based and theoretical approaches to explore digital cultures, investigating how technical environments shape the political and social capacities of the everyday. He is based in Aotearoa, New Zealand. His work ranges from data infrastructures in Asia to migrant surveillance in the Pacific and far-right cultures online. He has recently completed a doctorate at Western Sydney University on algorithmic power.

COGITATIO

**Media and Communication (ISSN: 2183–2439)**
**2020, Volume 8, Issue 2, Pages 280–290**
**DOI: 10.17645/mac.v8i2.2807**

Article

# Reflections upon the Privacy in the Converged Commercial Radio: A Case Study of *Royal Prank*

Grażyna Stachyra

Institute of Communication and Media Studies, Maria Curie-Skłodowska University, 20-080 Lublin, Poland;
E-Mail: grazyna.stachyra@poczta.umcs.lublin.pl

Submitted: 15 January 2020 | Accepted: 11 May 2020 | Published: 23 June 2020

**Abstract**

This article focuses on the problematic consequences of shifting boundaries of converged radio practices for individual privacies. Holding that privacy is constructed through the interrelated information practices of both individuals and their mediated surroundings, it addresses radio as a previously intimate and privacy friendly medium. The case of the *Royal Prank* call by the Australian 2DayFM radio station demonstrates how contemporary converged radio practices affect the privacies of unintended participants in their shows. In December 2012, Jacintha Saldanha, nurse of London's Royal King Edward VII Hospital committed suicide after two Australian radio presenters had made a prank phone call pretending to be Queen Elizabeth and Prince Charles concerned about the state of Duchess Kate's health, who was expecting her first child. The case identifies three conditions, each with implications on privacy. First, digitization renders radio content archivable and repeatable. There is a second life of radio programs keeping available information about any people involved. Secondly, the division of radio related labour leads to a lack of journalistic responsibility for respecting privacy standards. Broadcasters feel no need to be sensitive regarding the consequences of disseminated material, as commercial and legal staff decide on that. Finally, legal frameworks continue to apply legacy radio privacy measures and do not correspond to these new working conditions, as the reactions of the Australian supervisory authority show. In consequence, the case of the *Royal Prank* call demonstrates the impossibility to fight individual privacy when one is unintentionally involved in radio shows.

**Keywords**

commercial radio; convergence; media supervision; privacy; radio station; radio show; Royal Prank

**Issue**

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

## 1. Theory

The convergence of radio with other digital media was a revolutionary process that evoked substantial changes in radio production. The outline of any new concepts of privacy (not yet fully defined) emerged as part of these changes.

When radio broadcasting was first introduced in the early 1920s, the broadcast signals did not stop at national borders. An increasing number of listeners were soon enjoying programs from far away (Ala-Fossi, 2016, p. 280), "but when TV was introduced after WWII, it was in practice a 'medium without a public"' (Fickers, 2006, pp. 16–18). The competition for the auditorium had begun. Over the years, the radio had lost its monopoly status, but its essence remained untouched.

In the following decades new technologies emerged (i.e., satellite radio, internet), so the radio signal found new transmission channels and flowed via fibre-optic cable. The media convergence (Jenkins, 2008) turned out to be a real revolution for the radio. It changed the way of radio communication and brought the radio onto the path of online technology. Radio websites became a tool for providing extended information on the regulations of competitions, awards, radio people, the history of radio stations, etc. Radio stations started to visualise fragments of the program and put them online. Gradually, broadcasters began to publish recorded fragments of programs online, whereas podcasts were born.

Convergence was quite broadly described by R. Silverstone, who pointed out several of its aspects—from technological innovation to 'consequential convergence in patterns of use' by consumers (Silverstone, 1995, p. 11). Many studies have invoked this convergence concept, as they have analysed changes in news production practices within media organisations of which they are "seeking to distribute across different media platforms" (Preston & Rogers, 2013, p. 249), including the implications for the status of journalists (Preston, 2009). The concept of convergence implies a blurring of the distinctions between what were previously separate communication services and functions (de Sola Pool, 1983). Convergence as the "combination of technologies, products, staff and geography amongst the previously distinct provinces of print, television and online media" (Singer, 2004, p. 3), opened the space for 'transmedia storytelling.' The term primarily identified in the 1990s (by authors in different areas), was coined by Henry Jenkins (2003) as a process "where integral elements of a fiction get dispersed systematically across multiple delivery channels to create a unified and coordinated entertainment experience" (Sousa, Martins, & Zagalo, 2016, p. 119). That is why the content accessible by portable devices over the mobile Internet can be considered in a quite literal sense as 'remediated' by one medium in another (Dwyer, 2015, p. 17). Convergent media industries are merging and diffusing across media platforms together with their transmedia audiences, using multiple screen devices and mobile interfaces (Dwyer, 2015, p. 13) The media content is often 'optimised' for the web, modified for being accessed by mobile devices according to the motto: "Choose the best media to launch a story and the best flow between media" (Meier, 2007, p. 7).

For the radio one of the new ways to 'flow between media' meant the birth of the podcast. The term 'podcasting' was introduced in 2004 by the BBC journalist Ben Hammersley (Bonini, 2015, pp. 21–30). Podcasting is both producing podcasts (audio files, sometimes also video), as well as the technology to download them via an RSS reader. This allows the storage of podcasts on a computer, MP3 player, or mobile phone using free software such as iTunes or Juice. Podcasts migrated from radio. The BBC was a pioneer of this trend in 2004, making fragments of radio programs (podcasts) available on the BBC website. Podcasts can be listened to with a time shift (Dubber, 2013, p. 58). Todd Cochrane describes podcasting as "walkaway content" operating outside of the radio (Berry, 2006, p. 145). Siobhan McHugh (2012, p. 40) views podcasting as the incarnation of radio narrative forms. Richard Berry (2016, p. 5) claims that podcasts should be considered as radiogenic practices or occurring within the radio industry. Some online stations broadcast short cyclic episodes of programs and call them podcasts. In most cases however, radio stations place podcasts on their websites or podcast platforms.

Podcasting has brought many benefits to radio listeners, but "the human being is not quasi-automatically 'prepared' for the effects of every new technology" (Köchler, 2017, p. 9). Podcasting changed the perception of people's privacy. Modern radio is a part of the integrated media industry, in which the attractiveness of content is a primary goal and the possible violation of third-party privacy is part of the cost. Radio is winning the 'game of privacy' played between the media, public figures, politicians, and celebrities. The media need attractive protagonists in the public sphere. Likewise, they also need the media to exist in a public sphere. The problem with the privacy limitations is that those limits are very fluid and not defined properly. There is sort of 'grey area,' where the privacy of some actors is not properly protected. They become the victims of 'collateral damage,' as a result of the game that the media industry plays with public figures and the audience. This article illustrates one of such cases.

## 2. Transformations of the Radio as the Private Medium

The first explicit articulation of privacy was connected with media. As photography was emerging, whereby opening possibilities for publicising the private image of people via newspapers, Samuel Warren and Louis Brandeis in 1890 defined privacy as the right to "being left alone" or "being free from intrusion" (Tavani, 2013, p. 135). Gradually however, interpretations of intrusion concerned the right to determine what others should know about someone, control the possibility of identifying a given entity by others, and finally "one's ability to restrict access to and control the flow of one's personal information" (Ess, 2013, p. 72; Tavani, 2013, p. 136). Many researchers have shown that technology or politics have an impact on privacy. This is true, but apart from that there are certain business practices in the realm of journalism which can take away this control and violate the right to privacy.

It seems that the invention of the radio at the beginning of the 20th century guaranteed this control to the human being. Music, voices of announcers, and the theatre of imagination were introduced to the safe atmosphere of the private home. Because radio was a heavy piece of furniture, it was mainly listened to in the family circle. The 'radio at home' was associated with a specific broadcasting mode in which the value of the listener's comfort was simply receiving the broadcast. Habermas (1996) commented that:

> The threshold separating the private sphere from the public is not marked by a fixed set of issues or relationships but by different conditions of communication. Certainly, these conditions lead to differences in the accessibility of the two spheres, safeguarding the

> intimacy of the one sphere and the publicity of the other. (p. 366)

That is why the radio strategy of building relationships was achieved by creating an atmosphere of closeness and uniqueness of the announcer's contact with the listeners. In the history of the radio, this stage can be called "intimacy radio" (Peters, 1997, pp. 5–16). In 1956 Donald Horton and Richard Wohl claimed "that while striving to build close relationships with the audience, the performers [via TV or radio] employed a mode of communicating 'for someone' by using devices such as rhetorical questions, voice modulation, or phrases of direct address" (Horton & Wohl, 1956; Stachyra, 2017, p. 94). Although the radio reached an individual listener in remote parts of the world, it also evoked a sense of unity with other people listening to a specific program at the same time. It was therefore, a medium of both individual (private) and collective experience.

Gradually, radio's message resounded in factories (especially by mobilising workers during painstaking assembly-line work during WWII), or places of public utility. The 'exodus' of the radio from confined spaces was possible—from the 1960's—with the invention of transistor radio. Particularly in the US, the talk format began to gain popularity, promoting "ordinary topics" in radio discourse. Talk radio made headlines in the US in the mid-1980s, when Howard Stern gained both fame and the nickname "shock jock" (Douglas, 2002, p. 486). At the end of the 1980's, the availability of mobile phones to private people increased rapidly. Contact with the radio had become easier than ever, so the broadcasters encouraged their audience to use many of new forms of contact. It resulted in more news and opinions, fast and often unverified news, and a growing number of 'prosumers.' Sensationalism appeared as a production trend in commercial stations. Controversial topics attracted the attention of listeners.

Access to mobile phones also facilitated the implementation of the joke-call genre, in which journalists (hosts, DJs, etc.) would call random or deliberately selected 'guests' and impersonate various people. They engaged the interlocutors in an intrigue which in the end simply means to be funny. The genre has a long radio history as it has been present on air since the 1940s, when the first gags in the series of *Candid Microphone* appeared. The entertainment convention of the prank-call (also called joke-call) promotes the journalists playing various roles and making a voice creation or preparation of a person's speech. These were the beginnings of radio tabloidization. The entertainment target began to justify the intrusion of a radio microphone into the safe sphere of a human being.

The consequence of radio-wide availability and broadcast duplicability on many platforms is a significant change in the context of privacy. On the analogue radio, the privacy of people appearing on air was obvious due to the lack of image (no recognition of the speaker's identity), but also the one-time broadcast. On-air events did not remain in the listener's memory because they could not be repeated. On analogue radio, joke-calls sounded once. But the latest technologies and convergence contributed to the reproduction of jokes on the internet. What's more, presenters' behaviour became bolder according to the tabloid rule of sensationalism. In 1995, Canadian satirist journalist Pierre Brassard called Queen Elizabeth II, claiming to be Canadian Prime Minister Jean Chrétien. He persuaded her to record support for Canadian unity (the joke took place just before the separatist referendum of the Quebec province). The conversation was broadcast a few hours later on the Montreal radio CKOI FM as part of the satirical program *Le Bleu Poudre*. The palace called the prank "irritating and regrettable" (Lyall, 2012).

In 2003, two hosts of the Spanish-language radio WXDJ-FM in Florida, made a direct call to the president of Venezuela, Hugo Chavez. They provoked him to the alleged dialogue with the president of Cuba, Fidel Castro, whose voice was prepared from various media presentations. After a while, they revealed themselves and had fun on the air. What is more, a few months later, they did the same, this time calling Castro live and using the cooked-up statements of Chavez. When they appeared on air—they heard Castro's insults ("Miami radio fined for Castro hoax," 2004).

Convergence enabled the emigration of the *Royal Prank* 'outside' the radio to other media. That is why all the media almost simultaneously became recipients of the prank. The mediatised 'actor's' statements create the social context of the *Royal Prank*. Mediatisation is a set of transformations in the nature of contemporary social order, linked to the affordances and uses of media (Couldry, 2014). Therefore, the facts of the *Royal Prank* as the consequences of radio order under the convergence, the social context created by the 'actors' (entities) involved in this case and commercial radio legislation will be interpreted in this perspective.

Contemporary radio convergence makes the recordings (like those mentioned above) always available online. Search engines link to radio podcasts. We can say they 'immortalise' prank calls. It can be expected that constantly rediscovered joke-calls bring fans to radio stations. The heroes of the jokes mentioned above were public figures. But how strong is the 'right to be forgotten' in the case of civilians who are random heroes of the prank? The quote by Andrus Ansip, vice-president designate for the digital single market at the European Commission, sounds remarkable: "The European Court of Justice did not say that everybody has the right to be forgotten. 'Right to be forgotten' has to stay as an exception" (Dwyer, 2015, p. 47). This right is even more profound in the context of the accidental violation of privacy on the radio. This is due to the depersonalization of radio podcast production. Presenters must subordinate their behaviour to the overriding interests of the station. Even if it means an attempt on the privacy of third parties used in the recording. The *Royal Prank* is the case analysed here. It illustrates three factors that combined contribute to the present state of privacy protection in the modern radio: technology, production process, and insufficient legal regulations.

## 3. The Case of the *Royal Prank*

On December 2nd, 2012, Catherine, Duchess of Cambridge, was admitted to King Edward VII Hospital in London because of nausea. The media interest in this fact was enormous and somehow forced a statement by her husband Prince William, that the duchess was expecting their first child. On December 4th, at around 5:30 in the morning London time (GMT) and 4:30 p.m. Sydney time (AEST), the hosts of the Hot30 Countdown entertainment program of the Australian station 2DayFM, Mel Greig and Mike Christian, called the hospital claiming to be Queen Elizabeth II and the Prince of Wales ("Royal prank scandal," 2013). Nurse Jacintha Saldanha, who happened to be at the reception desk, answered the phone. There was no duty officer at the headquarters at night. Mel Greig overplaying a British accent asked for a conversation with Duchess Kate. Jacintha Saldanha herself did not reveal any secrets of the hospital or the patient, but switched the call to the nurse on duty with the Duchess, who provided confidential information about her health. Mike Christian joined the conversation, imitating the barking of corgi dogs, and then (as the Prince of Wales), asking when it would be possible to visit the Duchess in the hospital.

The joke was broadcast the next day (December 5th) with the consent of the station's lawyers. As a leading entertainment group, Southern Cross Austereo (SCA; 2DayFM's parent company), immediately spread the joke. The next day it was in the news headlines of all media in Australia and the world.

On December 7th, Jacintha Saldanha "was found hanged in her apartment in the nurses' quarter of the hospital in Marylebone, central London" (Laville & Davies, 2012).

## 4. The Method

According to methods in contemporary media and communication research, many options for 'producing' content and distributing it result in "a complexity, a flux, and difficulties in how to capture it" (Kubitschko & Kaun, 2016, p. vi). Thinking about the privacy transformations in contemporary radio, I have chosen the case study method as optimal. Although frequent criticism of case study methodology is that its dependence on a single case renders it incapable of providing a generalizing conclusion (Tellis, 1997), qualitative case studies are yet "an intensive, holistic description and analysis of a bounded phenomenon" (Miles & Huberman, 1994, p. 25; Yazan, 2015, p. 134). "It is a research strategy that focuses on understanding the dynamics present in a distinctive case" (Eisenhardt, 1989, p. 534).

According to Robert Yin's definition (2002, pp. 13–14), case is "a contemporary phenomenon within its real-life context"; an inquiry that investigates the case by addressing the 'how' or 'why' questions concerning the phenomenon of interest. Robert Stake and Robert Yin (Baxter & Jack, 2008, p. 545) base themselves on a constructivist paradigm which is itself built upon the premise of social construction of reality (Searle, 1995). In general, constructivism seeks to explain how norms, principles, institutions, and discourses create social reality or, in other words, how these 'social contexts' affect social and political processes and, generally, the policymaking process. The basic premise of constructivism is that social reality is the result of an agreement between people, i.e., social reality is socially constructed. In this sense, individuals or entities act following their intersubjectively-shaped images of surrounding reality.

As Yin (2003) states, a case study design should be considered when we want to cover contextual conditions because we believe they are relevant to the phenomenon under study. The case study chosen in this article points to the impact of radio convergence on the perception of individual privacy. The social context of the case is constructed by 'actors' involved: Radio DJs and management; institutional supervisory bodies of the radio; the royal family environment and some of its members; hospital representatives.

In this article I use an 'intrinsic' type of case study. Stake (1995) suggests taking this approach "when the intent is to better understand the case…because in all its particularity and ordinariness, the case itself is of interest" (Baxter & Jack, 2008, p. 549). According to Stake (1995), documents could be the sources of evidence. In my analysis of the *Royal Prank*, newspaper articles and online news were reviewed. They were retrieved from: *BBC*, *ABC*, *CNN*, *The Guardian*, *Daily Mail*, *Daily Telegraph*, and *The New York Post* in the period between December 2012 and December 2015. The keywords used for the search were: 'Royal Prank' and 'Jacintha Saldanha.' Furthermore, the online privacy guidelines of the British Office of Communications (Ofcom) and the Australian Communications and Media Authority (ACMA) were studied. A review of available documents was used as a data gathering tool here while its interpretation was the way to analyse the data collected. This allowed an answer to be provided for the given research questions:

> Research Question 1: How did the process of creating the *Royal Prank* call influence its final outcome?
>
> Research Question 2: What is the social context of radio broadcaster responsibility for the privacy of other parties?
>
> Research Question 3: How do the privacy protections of third parties work in legal terms, with regard to radio prank calls?

## 5. The Social Context of the *Royal Prank*: Media Reactions before and after Jacintha Saldanha's Death

The social reception of the *Royal Prank* can be divided into two stages. The first stage (until Jacintha Saldanha's suicidal note revealed) was mostly focused on the prank, Duchess Kate, and her privacy. The latter stage began with the news of a nurse's suicidal death, and from this moment the discussion shifted to her privacy and, in more general terms, to the questions of journalistic boundaries and responsibilities.

### *5.1. Stage One—The Beginning*

2DayFM is a part of the SCA group that controls radio and television stations around Australia. At the time of the prank call in 2012, it was one of the most popular radio stations with 259,000 listeners (Wilding, 2015). The *Royal Prank* materials were recorded on the 4th of December and broadcast on-air on the 5th of December 2012. Then, the journalists themselves started promoting the recording on social media. To his 3,700 followers, Mike Christian tweeted: "Not sure how it happened, but called Kate Middleton's hospital pretending to be The Queen and they PUT US THROUGH!!" (McMillen, 2013). On Facebook, he wrote: "The only bad thing about our Royal Prank is knowing that I will NEVER EVER top this" (McMillen, 2013). Mel Greig told *The Adelaide Advertiser*: "This is by far the best prank I've ever been involved in….It's definitely a career highlight" (McMillen, 2013). "The hashtag #royalprank was retweeted more than 15,000 times on Twitter after the radio station began promoting the call" (Mendoza, 2012). Within two days, at least 5,000 joke links were created on the web. "The annual turnover of SCA Company for the 2011–2012 financial year was AUD $273.6 million (US $247 million). The wording of that portentous SCA press release announcing the 'biggest Royal Prank ever' certainly may not have been hyperbole" (McMillen, 2013).

The Duchess's entourage accepted the joke with leniency. Just after the broadcast, a spokesman for William and Kate stated that "he would be making no comment on the hoax call" ("Royal pregnancy," 2012). Royal commentator Robert Jobson said he "did not believe the radio call had been intended as a serious invasion of (the duchess') privacy" (Mendoza, 2012). "The palace has refused to comment about the embarrassing hoax saying they were leaving responses to the hospital" (Miranda, 2012). On December 6th, two days after the joke, when asked for comment as a future grandfather, Prince Charles replied: "How do you know I'm not a radio station?" (McMillen, 2013). In other words, Prince Charles did not consider the joke a violation of the privacy of the royal family and took a rather humorous approach to the situation.

The British online press has hit an alarming tone. The press criticised presenters, demanding their dismissal and the suspension of the broadcast. Above all, however, it emphasised the demand for an apology to the Duchess "for invading her privacy so egregiously, and deceptively" (McMillen, 2013). On December 5th, *The Telegraph* asked the question: "How is it OK to scam a hospital into telling you about a pregnant woman's condition?…*The Sun* called the presenters "brazen" and *The Daily Mail* reported on Buckingham Palace's fury at the privacy breach" (Miranda, 2012). The overtone of the 2DayFM broadcast was pure entertainment. The Facebook post of the station under the recording told us to "listen to the prank that the world is talking about. Can you believe Mel and MC got away with these dodgy accents?" (Mendoza, 2012).

### *5.2. Stage Two—Aftermath*

After the death of Jacintha Saldanha, social media was constantly duplicating updates about the prank: "The Twitter account for radio host Michael Christian (@MContheradio) had included five updates about the prank in the morning of the nurse's death….The hashtag #royalprank continued to be used after news of the nurse's death" (Mendoza, 2012). "More than seven hours after Saldanha's death, 2DayFM's website was still plugging its royal scoop" (Rayner, 2012).

It was only Jacintha Saldanha's suicide and her farewell letter in which she blamed the presenters and demanded: "make them pay for my mortgage" (Smyth, 2013) that started the discussion about the legal context of the *Royal Prank*. Moreover, the legal investigations were initiated both in Great Britain and Australia. One in connection to the nurse's death was led by the coroner, and another in regard to professional standards of broadcaster and its staff was introduced by ACMA.

The *Royal Prank* was broadcasted without consent of the people involved—that was one of the conclusions. Rhys Holleran (chief executive of SCA) claimed that "the station had attempted to contact King Edward VII Hospital no less than five times before broadcasting" (Rayner, 2012). The hospital spokesperson accused the station, in turn, that on its behalf even a single person "did not speak to anyone in the hospital's senior management or anyone at the company that handles our media inquiries" (Rayner, 2012). The investigation showed that indeed "four calls—the longest lasting 45 seconds—were made by the radio station to the hospital….They were terminated by the recipient, who was almost certainly Saldanha" (Davies, 2014a). The coroner, during the trial following the death of Jacintha Saldanha in London, stated: "If she did take those calls, I find it inconceivable she would have consented, as a participant in the call, to its broadcast" (Davies, 2014a). One can assume that 2DayFM was only formally trying to get permission to broadcast a joke, stubbornly calling the reception of the hospital instead of trying to get through to its management. It is obvious that obtaining such permission from the hospital as an institution of social trust was impossible. John Lofthouse, the hospital's chief executive, stated:

"This was a foolish prank call that we all deplore…it was technically…a breach of patient [Duchess] confidentiality" ("Royal pregnancy," 2012).

The *British Daily Mail*, quoting the Indian press, reported that "Jacintha Saldanha had attempted suicide twice before…during a family visit to India" (Taher, 2012). The owner of 2DayFM—SCA—published a statement stating that "neither police nor the hospital had publicly blamed the radio station for Saldanha's death" (Mendoza, 2012). But the nurse realized that the whole world knew about the joke: "A police search of her laptop showed she researched suicide prevention sites, and news reports of the hoax" (Davies, 2014a). Saldanha did not have the courage to appear at work: "I don't know how to face the bosses tomorrow. I feel so ashamed of myself" (Davies, 2014b). She couldn't even talk to her husband about it: "They spoke several times that week, but she did not tell him or the kids anything about it" (Palmeri, 2012). Jacintha Saldanha's emails disclosed during the investigation testify that she was overwhelmed with responsibility for her friend to whom she transferred the received prank call: "It's all my fault and I feel very bad about this getting you involved….At the moment in time, with that voice, I couldn't even think of anything else" (Davies, 2014a). Jacintha Saldanha was afraid of professional consequences, too. She wrote to her superior: "I feel very sorry for breaking security, I am ready for any punishment" (Davies, 2014a). Chief executive of the hospital John Lofthouse condemned the joke, stating that "nurses were trained to care for people, not to cope with journalistic trickery" (Rayner, 2012), but there was no public stance of superiors. Lofthouse also commented that "some senior managers thought both nurses should be disciplined, but his view, and that of the matron, was that the nurses were victims and categorically they would not be disciplined" (Davies, 2014b). As the investigation showed, the supervisor did not find time to reply to the emails of the concerned nurse (Davies, 2014b).

## 6. Modern Radio Production and the Politics of Privacy Protection

On modern radio in democratic countries, the policy of privacy harmonises with the principles of the liberal or democratic corporatism model of Hallin and Mancini (2004, pp. 34–35). According to this model, autonomy is a key determinant of professional journalists. They should achieve the highest standards through self-improvement and have responsibility for the accuracy of published content. However, it should take into account the fact that media products are often the result of collective actions. That, to some extent, may disturb the autonomy of individuals. Journalistic autonomy is determined at the legislative level of a country, through legal acts like media law, legal regulations for broadcasters, etc. On a lower level of co-regulation, the creation of norms is done with active participation (between) the state organizations and media/owner. In addition to these guidelines, radio stations may (but do not have to) draw up internal editorial rules: *self-regulation*, that require journalistic diligence to comply with good radio practices (Dobek-Ostrowska, 2019, pp. 48–49). This strategy is a well-known voluntary form of "employing ethics in practice in journalistic groups, mainly associated with television, radio, the Internet, social media, advertising, etc. Media institutions freely and upon their own initiative, impose restrictions on themselves or adopt rules of conduct" (Jakubowicz & Sükösd, 2008, p. 37). In many countries around the world the radio market consists of three sectors: private, public, and community. On one hand, this diversity supports the autonomy of journalists, but on the other, it restrains some of this diversity. This results from the differences in political systems, cultures, or the development of civil society. Restrictions on journalistic autonomy arising from the commercial nature of radio stations, in which employees primarily seek for an attractive content, are particularly important. In the case of commercial broadcasters, there is a preference towards financial factors in broadcasting policies. Therefore, the protection of privacy under *self-regulation* may be difficult, due to the tabloid model of communication. Following controversial, sensational and entertainment themes does not go hand in hand with applying internal restrictions in the form of a code of ethics.

Especially at the *self-regulation* level, radio stations are guided by principles consistent with the program strategy and institutional interest. In the case of commercial stations, especially those which are elements of media corporations (such as 2DayFM), the decisive factor is the attractiveness of the message and its 'market' potential. The message becomes a product for sale. In the era of converged radio, the *Royal Prank* could function as a web podcast. The *Royal Prank* was recorded, re-edited, and then put on broadcast on *Hot 30 Countdown* six hours after the phone call to the hospital had been made. The *Royal Prank* was a ripped fragment of the broadcast. The act of recording material by journalists and its post-production were separated. "The call was established by the station's PAPX system, linked to the studio via an answering device known as Phone Box, then recorded and played out through equipment known as Voxpro" (Wilding, 2015). Because the prank itself fit the call-joke genre, and its content was very attractive, it became part of the broadcast of *Hot 30 Countdown*, which was very popular among listeners.

The fragmentation of the original broadcast and its promotion have important implications in the context of privacy policy. Each radio station should obtain permission from a person whose voice is used in the recorded material prior to its broadcasting. In case of radio quiz shows and competitions, the listeners first agree to the recording and its use (including online and on-demand channels without time restrictions).

During their live program, the pair of DJs—Greig and Christian—broadcast a fragment (the *Royal Prank*) which was edited by someone else. In this way, adequate protection of the privacy of individuals affected by the prank was not within their responsibility. The responsibility was taken over by station lawyers, who allowed the broadcast to take place, ignoring Mel Greig's doubts, who admitted that she should have "tried harder to stop the prank from airing" (Davies, 2014a). At the same time, Greig confirmed her own thoughtlessness of the participant in the process of 'external' radio production, i.e., previously recorded and subject to post-production before being broadcast on air: "There's a whole team of people that work with us. We just go on and keep recording stuff or doing other prep….We do that and leave it for everybody else to deal with" ("Royal prank scandal,'' 2013).

The presenters of the *Royal Prank* themselves primarily lacked 'soft' guidelines for ethical behaviour at work. The 2DayFM station naively explained: "they fully expected hospital staff to hang up on them within seconds after picking up on their 'silly English accents"' (Duell, Andrews, Greenhill, Shears, & English, 2012). Mel stated that "we obviously wanted it to be a joke" (Duell et al., 2012). Mel and Mike however, lacked journalistic reflection, which should stop them from making a phone call to the hospital for a joke, where the Duchess was concerned about the fate of her early pregnancy, and was additionally overwhelmed with the expectations of her as the mother of the future heir to the throne. *Self-regulation* principles would require interrupting the conversation and revealing the perpetrators of the joke at the right moment of the recording. From an ethical perspective, it seems obvious that the DJs should have stopped the conversation before the nurse revealed the intimate details of Duchess Kate's well-being. One can assume that they did not reveal themselves, because they did not feel that they had crossed any ethical boundaries. They lacked a *self-regulation* ethics code that required moral virtues. Virtue ethics thereby foregrounds the importance of "moral wisdom…and the questions of what sort of person I should be" (Ess, 2013, p. 241). Instead, private information on patient care was disclosed, which resulted in media around the world buying the *Royal Prank*. Thus, the joke became a scandal because it forced the institutional response of the hospital, defending itself against allegations of poor protection of patient safety. And since there was a protocol of conduct in this case, Jacintha Saldanha, who broke it and switched the call without verifying the phone number was first to blame, although the media did not make such a statement explicitly.

As a result of an investigation of ACMA it turned out that 2DayFM broke the 'commercial radio code of practice' in Australia (Wilding, 2015). This rule also applies in the British broadcasting law, including in the Communications Act of 2003 and the Broadcasting Act of 1996 (Ofcom, 2017). The station intentionally broke the commercial radio code:

> By broadcasting the words of identifiable persons in circumstances where those persons: were not informed in advance that their words may be broadcast, would not have been aware that their words may be broadcast, did not give their consent to the broadcast of the words. (Wilding, 2015)

The station's decision to broadcast the *Royal Prank* without the consent was therefore a play with privacy policy. A media law specialist at Sydney University, Professor Barbara McDonald, said that "2DayFM knew they should be getting consent (to air the interview) and they failed to. It almost showed they knew (what) they had to and they didn't and then they decided to run the risk" (Rourke, 2012). The aforementioned decision not only violated the law, but also Jacintha Saldanha's personal rights. The presenters joke provoked her improper professional behaviour, exposing her to the consequences from her employer. ACMA, in a report published on 20th April 2015, investigating whether the broadcaster had committed an offence that violated the terms of its licence, stated:

> The broadcast used the deception of the prank to engage with the Employees in a way that was personally degrading and humiliating and was likely to reduce their professional standing….Even if the material obtained as a result of the prank was unexpected, once it was obtained the decision to broadcast it—some four and a half hours after it was recorded—was made deliberately by the licensee and in circumstances in which the licensee could have assessed the likely impact of its broadcast on the Employees. (Wilding, 2015)

The prank jeopardised the nurses' good name as "their voices were clearly audible…the content broadcast was…highly newsworthy and its publication detrimental to the interests of the employees, the employees were identified by the hospital because of the prank call" (Wilding, 2015).

However, in ACMA's opinion, 2DayFM did not break the 'privacy code' because:

> There was no breach of the rule regarding offence against 'generally accepted standards of decency'….Nor did it breach the rule concerning the use of 'material relating to a person's personal or private affairs, or which invades an individual's privacy.' The privacy rule only applies to news and current affairs programs and the ACMA agreed with 2DayFM that Summer 30 was not such a program. (Wilding, 2015)

The legal loophole in the 2DayFM privacy policy is therefore due to the nature of the entertainment program, although it is difficult to understand the selective treatment of the individual's rights to protect his or her privacy.

ACMA approved the legal provision about the lack of privacy protection of entertainment program participants, although 2DayFM repeatedly violated the code of good practice. It was reprimanded by a government supervisory body in 2009, after "a 14-year-old girl, brought on the show by her mother, was attached to a lie detector during a live broadcast and asked if she was having sex. She revealed that she had been raped" (Lyall, 2012). In turn, in 2011, "one of its hosts called a journalist a 'fat slag' and threatened her on the air" (Lyall, 2012). None of these offences ended in revoking of licenses for this type of 'entertainment.'

The station did not suffer any legal sanctions in connection with the emission of the *Royal Prank*. The ACMA only concluded that:

> The station will require all presenters, production and management staff to undergo a training program on their ethical and legal obligations….A further license condition has also been applied for three years, ensuring the station does not broadcast the words of an identifiable person unless they've been informed in advance. (Whitbourn & Lallo, 2015)

## 7. Conclusions

The case study of *Royal Prank* illustrates three aforementioned main issues with implications for the privacy protection. First, it is the technical aspect or digitization of radio content and convergence with other media. Then, there is division of radio-related labour, leading to a lack of professional responsibility for respecting privacy standards. Last but not least, there is a lack of proper legal tools to deal with the deficiencies in privacy protection, which are brought by the first two factors. In the case of the *Royal Prank* all of them result in the impossibility to protect individual privacy of a person who is unintentionally involved in a radio show.

### *7.1. Technology and Convergence*

The study points to the impact of radio convergence on the perception of individual privacy. The podcast nature of broadcasting in convergent radio means that it reaches 'beyond the radio,' to random online recipients as an abstracted fragment of a radio show. It gains 'an afterlife' on the Internet. The sound is provided with the images of the presenters in the studio and placed on social media to entertain the audience, at the price of discrediting people who are treated merely as the unaware figures playing their parts for the benefit of the show. The case uncovers the loss of editorial control over the program and lack of journalists' responsibility for the final outcome. The case also shows how duplicating previously recorded excerpts on the Internet opens the space for violating the individual's right to privacy.

### *7.2. Radio Production*

The case study shows how the actions of both Radio DJs and management evoked mediatised reactions of institutional supervisory bodies of the radio, the Royal Family environment and hospital representatives. The Australian presenters were tempted to extend the prank's conversation and make it more attractive for social media. Self-regulation principles would require interrupting the conversation and revealing the perpetrators of the joke at the right moment of the recording. Due to this fact, the interrogated nurse could not react spontaneously and laugh (or not) at the joke along with others. She could not play a part in the game on equal terms. The radio and other media constructed the social context of the *Royal Prank*, where Jacintha Saldanha's 'right to be forgotten' was not respected. Repeating the *Royal Prank* in social media and discussing it via online media, on one hand ridiculed Jacintha Saldanha's language skills as an immigrant from India, on the other unintentionally emphasised her breaking the protocol. In a social context, Jacintha Saldanha was indirectly stigmatised for her violation of professional ethics.

### *7.3. Legal Issues*

The next step of the research was the interpretation of 2DayFM actions from the perspective of commercial radio legislation. That let the gaps in Jacintha Saldanha's privacy protection be exposed. 2DayFM broke the 'commercial radio code of practice' by broadcasting the prank without the consent of parties involved. Unaware people are recorded and drawn into the plot. Separating the process of recording and broadcasting material, frees journalists from responsibility for what they say on air. During the investigation, ACMA stated that 2DayFM did not break the 'privacy code' because of the entertaining convention of the *Hot 30 Countdown*. The lack of sufficient privacy protection for people who appear in the entertainment programs of commercial radio is the main negligence here. In the absence of their clear permission, the 'privacy code' should apply the same restrictions as in the case of news and current affairs programs. The position of the investigating authorities did not contain any indications for further action. The Crown Prosecution Service for England and Wales stated that "no further investigation is required because any potential prosecution there would not be in the public interest" (Wilding, 2015). In addition, the New South Wales Police Force and the Australian Federal Police, as a result of joint actions "found no breach of the Surveillance Devices Act 2007, the Telecommunications (Interception and Access) Act 1979, or any other Act" ("London hospital prank," 2015). These statements maintained the status quo in the Australian Privacy Policy for commercial radio in the form of the provision as "some codes offer express privacy protections only in the context of news and current affairs broadcasts" (ACMA, 2016). Among them is also the Commercial Radio Code of Practice and the Subscription Narrowcast Radio Code of Practice.

### *7.4. Summary*

Radio convergence provided 2DayFM with new tools to make a more attractive product and then sell it across many platforms. At the same time, it multiplied the damage to Jacintha Saldanha's privacy. The tragic finale fostered the investigations, but all the noted violations did not result in legal consequences for the parties involved.

The case of the *Royal Prank* also demonstrates a decrease of on-air intimacy and growing distance between the presenters and their audience. The *Royal Prank* is something more than just an isolated case of a radio prank. It illustrates the fragility of unintentionally involved humans who serve as mere puppets for the sole purpose of entertainment created by powerful media platforms.

## Conflict of Interests

The author declares no conflict of interests.

## References

Ala-Fossi, M. (2016). Why did TV bits and radio bits not fit together? Digitalization and divergence of broadcast media. In A. Lugmayr & C. Dal Zotto (Eds.), *Media convergence handbook—Vol. 1: Journalism, broadcasting, and social media aspects of convergence* (pp. 265—285). Berlin Heidelberg: Springer.

Australian Communications and Media Authority. (2016). *Privacy guidelines for broadcasters*. Canberra: Australian Communications and Media Authority.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, *13*(4), 544–559. Retrieved from http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf

Berry, R. (2006). Will the iPod kill the radio star? Profiling podcasting as radio. *Convergence*, *12*(2), 43–162.

Berry, R. (2016). Part of the establishment: Reflecting on 10 years of podcasting as an audio medium. *Convergence: The International Journal of Research into New Media Technologies*, *22*(6), 661–671.

Bonini, T. (2015). The 'second age' of podcasting: Reframing podcasting as a new digital mass medium. *Quaderns del CAC*, *41*(18), 21–30.

Couldry, N. (2014). Mediatization: What is it? In L. Kramp, N. Carpentier, A. Hepp, I. Tomanić Trivundža, H. Nieminen, R. Kunelius . . . R. Kilborn (Eds.), *Media practice and everyday agency in Europe* (pp. 33–39). Bremen: Edition Lumière.

Davies, K. (2014a, September 11). Jacintha Saldanha 'took blame' for Duchess of Cambridge prank call. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/sep/11/jacintha-saldanha-took-blame-prank-call-duchess-cambridge-australian-djs-inquest

Davies, K. (2014b, September 12). DJ apologises to Jacintha Saldanha's family as nurse's death ruled suicide. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/sep/12/jacintha-saldanha-death-suicide-prank-call-dj-apologises

de Sola Pool, I. (1983). *Technologies of freedom: On free speech in an electronic age*. Cambridge, MA: Belknap Press and Harvard University Press.

Dobek-Ostrowska, B. (2019). *Polish media system in a comparative perspective*. Berlin: Peter Lang.

Douglas, S. J. (2002). Letting the boys be boys: Talk radio, male hysteria, and political discourse in the 1980s. In M. Hilmes & J. Loviglio (Eds.), *Radio reader: Essays in the cultural history of radio* (pp. 485–505). New York, NY and London: Routledge.

Dubber, A. (2013). *Radio in the digital age*. Cambridge: Polity Press.

Duell, M., Andrews, E., Greenhill, S., Shears, R., & English, R. (2012, December 10). We're both shattered. My first thought was: Is she a mother? Radio hosts at centre of prank give self-pitying interviews. *Daily Mail.* Retrieved from https://www.dailymail.co.uk/news/article-2245727/Mel-Greig-Michael-Christian-interview-Were-shattered--thought-Is-mother.html

Dwyer, T. (2015). *Convergent media and privacy*. New York, NY: Palgrave Macmillan.

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review*, *14*(4), 532–550.

Ess, C. (2013). *Digital media ethics* (2nd ed.). Oxford: Polity Press.

Fickers, A. (2006). National barriers for an imag(e)ined European community: The technopolitical frames of postwar television development in Europe. In L. Hojbjerg & H. Sondergaard (Eds.), *European film and media culture, northern lights, film and media studies yearbook 2005* (pp. 15–36). Copenhagen: Museum Tusculanum Press.

Habermas, J. (1996). *Between facts and norms: Contributions to a discourse theory of law and democracy*. Cambridge, MA: MIT Press.

Hallin, D. C., & Mancini, P. (2004). *Comparing media systems: Three models of media and politics*. New York, NY: Cambridge University Press.

Horton, D., & Wohl, R. (1956). Mass communication and para-social interaction: Observations on intimacy at a distance. *Psychiatry*, *19*(3), 215–229.

Jakubowicz, K., & Sükösd, M. (2008). Twelve concepts regarding media system evolution and democratization in post-communist societies. In K. Jakubowicz & M. Sükösd (Eds.), *Finding the right place on the map: Central and Eastern European media change in a global perspective* (pp. 9–40). Bristol and Chicago, IL: Intellect Books.

Jenkins, H. (2003). Transmedia storytelling. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/2003/01/15/234540/transmedia-storytelling

Jenkins, H. (2008). *Convergence culture: Where old and new media collide*. New York, NY: University Press.

Köchler, H. (2017). Idea and politics of communication in the global age. In M. Friedrichsen & Y. Kamalipour (Eds.), *Digital transformation in journalism and news media media management: Media convergence and globalization* (pp. 7–15). Berlin: Springer.

Kubitschko, S., & Kaun, A. (Eds.). (2016). *Innovative methods in media and communication research*. Cham: Palgrave Macmillan.

Laville, S., & Davies, C. (2012, December 13). Jacintha Saldanha suicide note criticised hospital staff. *The Guardian*. Retrieved from www.theguardian.com/world/2012/dec/13/jacintha-saldanha-suicide-notes

London hospital prank: High Court backs authority's power to find 2Day FM radio presenters broke law. (2015, March 4). *ABC News*. Retrieved from https://www.abc.net.au/news/2015-03-04/high-court-backs-acmas-power-to-find-2day-fm-broke-law/6279276

Lyall, S. (2012, December 7). Prank call seeking royal family secrets takes horrifying turn. *The New York Times*. Retrieved from https://www.nytimes.com/2012/12/08/world/europe/nurses-death-stirs-sharp-criticism-of-royal-prank-call.html

McHugh, S. (2012). Oral history and the radio documentary/feature: Introducing the "COHRD" form. *Radio Journal: International Studies in Broadcast and Audio Media*, *10*(1), 35–51.

McMillen, A. (2013, August 2). The Royal Prank: The story behind the worst radio stunt in history. *BuzzFeed*. Retrieved from https://www.buzzfeed.com/andrewmcmillen/the-royal-prank-how-a-crank-call-became-a-tragedy

Meier, K. (2007). Innovations in Central European newsrooms: Overview and case study. *Journalism Practice*, *1*(1), 4–19.

Mendoza, D. (2012, December 11). Social media entwined in radio prank, nurse death. *CNN*. Retrieved from https://edition.cnn.com/2012/12/07/tech/social-media/radio-prank-suicide-social-media/index.html

Miami radio fined for Castro hoax. (2004, April 25). *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/americas/3657499.stm

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded source book* (2nd ed.). Thousand Oaks, CA: Sage

Miranda, C. (2012, December 6). Aussie radio hosts sorry for pretending to be Queen and Prince Charles in call to Kate's hospital. *The Advertiser*. Retrieved from https://www.adelaidenow.com.au/news/aussie-royal-radio-hoax-condemned/news-story/5b73e23a4e7c73df3aad351127693d54

Ofcom. (2017). Section eight: Privacy. *Ofcom*. Retrieved from https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code/section-eight-privacy

Palmeri, T. (2012, December 24). Nurse who killed herself after Kate Middleton hoax attempted suicide twice before. *The New York Post*. Retrieved from https://nypost.com/2012/12/24/nurse-who-killed-herself-after-kate-middleton-hoax-attempted-suicide-twice-before

Peters, J. D. (1997). Realism in social representation and the fate of the public. *The Public*, *4*(2), 5–16.

Preston, P. (2009). *Making the news*. London: Routledge.

Preston, P., & Rogers, J. (2013). Convergence, crisis and the digital music economy. In S. Diehl & M. Karmasin (Eds.), *Media and convergence management* (pp. 247–261). Berlin Heidelberg: Springer.

Rayner, G. (2012, December 8). 'Cruel' hospital hoax still playing on radio. *The Daily Telegraph*. Retrieved from https://www.telegraph.co.uk/news/9731359/Cruel-hospital-hoax-still-playing-on-radio.html

Rourke, A. (2012, December 10). Royal hoax station tried to contact hospital before broadcast. *The Guardian*. Retrieved from https://www.theguardian.com/uk/2012/dec/10/royal-hoax-station-contacted-hospital

Royal prank scandal: DJ Mel Greig settles dispute, resigns. (2013, December 5). *ABC News*. Retrieved from https://www.abc.net.au/news/2013-12-05/royal-prank-call-dj-settles-dispute-with-station/5138650

Royal pregnancy: Hoax call fools Duchess of Cambridge hospital. (2012, December 5). *BBC News*. Retrieved from https://www.bbc.com/news/uk-20610197

Searle, J. R. (1995). *The construction of social reality*. New York, NY: Free Press.

Silverstone, R. (1995). Convergence is a dangerous word. *Convergence: The international journal of research into new media technologies*, *1*(1), 11–13.

Singer, J. B. (2004). Strange bedfellows? The diffusion of convergence in four news organizations. *Journalism Studies*, *5*(1), 3–18.

Smyth, S. (2013, April 28). Jacintha Saldanha suicide note over Kate Middleton hospital prank call: 'Holds radio DJs responsible.' *Daily Mail*. Retrieved from www.dailymail.co.uk/news/article-2316055/Jacintha-Saldanha-suicide-note-Kate-Middleton-hospital-prank-holds-radio-DJs-responsible.html

Sousa, M. N., Martins, M. L., & Zagalo, N. (2016). Transmedia storytelling: The roles and stakes of the different participants in the process of a convergent story, in divergent media and artefacts. In A. Lugmayr, C. Dal Zotto (Eds.), *Media convergence handbook—Vol. 2: Firms and user perspectives* (pp. 117–137). Berlin Heidelberg: Springer.

Stachyra, G. (2017). Podcasting as audio technology. Development prospects. *Media Studies*, *68*(1), 1–17.

Stake, R. E. (1995). *The art of case study research*. Thousand Oaks, CA: SAGE.

Taher, A. (2012, December 22). Royal nurse found hanged after taking DJs' hoax call about pregnant Duchess of Cambridge had tried to kill herself twice before last year. *Daily Mail*. Retrieved from https://www.dailymail.co.uk/news/article-2252290/Jacintha-Sadanha-Nurse-answered-hoax-Duchess-Cambridge-attempted-kill-before.html

Tavani, H. (2013). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (4th ed.). Hoboken, NJ: Wiley.

Tellis, W. (1997). Introduction to case study. *The Qualitative Report*, *3*(2). Retrieved from http://www.nova.edu/ssss/QR/QR3-2/tellis1.html

Whitbourn, M., & Lallo, M. (2015, July 17). Royal prank call: 2DayFM hit with tighter licence conditions. *The Sydney Morning Herald*. Retrieved from https://www.smh.com.au/national/royal-prank-call-2dayfm-hit-with-tighter-licence-conditions-20150717-gieel0.html

Wilding, D. (2015). The summer 30 royal prank call: Outcomes for Australian broadcasting regulation. *Journal of Media Law*, *7*(1), 92–107.

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134–152. Retrieved from http://www.nova.edu/ssss/QR/QR20/2/yazan1.pdf

Yin, R. K. (2002). *Case study research: Design and methods*. Thousand Oaks, CA: Sage.

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

## About the Author

**Grażyna Stachyra**, (PhD in Media Communication) is Associated Professor at Maria Curie-Skłodowska University in Lublin. She is former Vice-Chair of ECREA's Radio Research Section and Co-Editor of *Radio: The Resilient Medium* (Sunderland, 2014), *Radio Relations: Policies and Aesthetics of the Medium* (Cambridge Scholars Publishing, 2018). She is also Author and Co-Author of various articles dedicated to radio i.e., *The Radio Plays Games* (EJC, 2012), *Radio in the Workplace: A Liminal Medium between Work and Leisure* (Media Culture & Society, 2015), *Radio-Bodies as a Claim for Freedom: The Imagined Public Medium at the Majdanek Concentration Camp* (Media Culture & Society, 2019).

**Media and Communication (ISSN: 2183–2439)**
**2020, Volume 8, Issue 2, Pages 291–301**
**DOI: 10.17645/mac.v8i2.2846**

Article

# The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making

Yannic Meier [1,]*, Johanna Schäwel [2] and Nicole C. Krämer [1]

[1] Social Psychology: Media and Communication, University of Duisburg-Essen, 47057 Duisburg, Germany;
E-Mails: yannic.meier@uni-due.de (Y.M.), nicole.kraemer@uni-due.de (N.C.K.)
[2] Department of Media Psychology, University of Hohenheim, 70593 Stuttgart, Germany;
E-Mail: johanna.schaewel@uni-hohenheim.de

* Corresponding author

Submitted: 29 January 2020 | Accepted: 1 May 2020 | Published: 23 June 2020

**Abstract**
Privacy policies provide Internet users with the possibility to inform themselves about websites' usage of their disclosed personal data. Strikingly, however, most people tend not to read privacy policies because they are long and cumbersome, indicating that people do not wish to expend much (cognitive) effort on reading such policies. The present study aimed to examine whether shorter privacy policies can be beneficial in informing users about a social networking site's (SNS) privacy practices, and to investigate associations between variables relevant for privacy decision-making using one theory-based integrative model. In an online experiment, participants ($N = 305$) were asked to create a personal account on an SNS after being given the option to read the privacy policy. Privacy policy length and the SNS's level of privacy were varied, creating a 2 (policy length) × 2 (level of privacy) between-subjects design. The results revealed that participants who saw short policies spent less time on reading but gained higher knowledge about the SNS's privacy practices—due to the fact that they spent more reading time per word. Factual privacy policy knowledge was found to be an indicator for participants' subjective privacy perception. The perception and evaluation of the specific SNS´s privacy level influenced the assessment of privacy costs and benefits. Particularly when benefits were perceived as high, self-disclosure was increased.

**Keywords**
online privacy; privacy calculus; privacy policy; self-disclosure; social networking site

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

## 1. Introduction

To fully enjoy the advantages of the Internet, users often need to disclose personal information to other users or to companies. According to the privacy calculus approach, decisions regarding such disclosure are based on the perception of disclosure benefits and privacy costs (Culnan & Armstrong, 1999), but they are also thought to be dependent on the subjective perception of the current privacy level (Dienlin, 2014). While benefits of sharing personal information often occur immediately and are easy to grasp (because they are the main reason for disclosure), users appear to have difficulties in predicting privacy costs, as they are often abstract and occur with a time delay (if they occur at all). Usually, reading a website's privacy policy is one possibility for Internet users to inform themselves about the privacy costs that might arise from using the respective website. A privacy policy is a written statement about a website's privacy practices (i.e., the extent to which a website collects, uses, and disseminates user data). Since the EU General Data Protection Regulation (GDPR) came into force, website providers have been obligated to use easily understandable language in their privacy policies. However, the length of policies might still be based on companies' primary interest in safeguarding themselves, i.e., by providing the necessary information and thus acting lawfully, rather than on providing the best support for users (i.e., easy-to-read and understandable information). It has been found that only 13% of European Internet users fully read privacy policies, whereas 47% read privacy policies only partially and 37% never read privacy policies (European Commission, 2019). The main reasons stated for reading policies only partially or not at all were that they are too long and too complex (European Commission, 2019), indicating that many users are unwilling to expend much time and cognitive effort on informing themselves about a website's privacy practices.

To address this problem, the first aim of the current article is to focus on the length of privacy policies by investigating whether short policies can be more effective in informing users. The second aim is to test different assumptions relevant for online privacy decision-making that stem from two approaches combined into one integrative model. These approaches are the privacy process model (Dienlin, 2014) and the privacy calculus (Culnan & Armstrong, 1999). The integrative model comprises knowledge about the policy's content, the subjective perception of the privacy level, and the assessment of privacy risk likelihood and disclosure benefits. In the present study, participants were asked to create a personal account on a social networking site (SNS), having been given the option to read one of the SNS's privacy policies beforehand. To gain a better understanding of the link between policy knowledge and the perception of online privacy, we varied not only the length of the privacy policies but also the SNS's actual level of privacy (privacy-intrusive vs. privacy-friendly), thus creating a 2 (policy length) × 2 (level of privacy) between-subjects design.

## 2. Literature Review

### *2.1. Privacy Policy Length*

According to the limited capacity model of motivated mediated message processing (LC4MP), people have limited available cognitive resources to process messages (Lang, 2000). The amount of available resources to process particular messages depends on the individual. Generally speaking, however, simple messages should lead to a higher likelihood of being processed compared to complex messages, since fewer (cognitive) resources are required and people are thus more easily motivated to engage in message processing (Lang, 2017). This approach can serve as an explanation for why few Internet users fully read privacy policies. Many people believe that privacy policies are too long and elusive (European Commission, 2019), implying that reading and understanding them requires cognitive or time effort. Deriving from this observation, the question arises whether shorter privacy policies that summarize the most relevant points of long policies might be more effective in informing users about the collection, usage, and dissemination of their personal data compared to the usually provided privacy policies. Short privacy policies might be more effective because people anticipate less time and cognitive effort and can more easily extract relevant information. Thus, one aim of the current study is to investigate whether users who are confronted with short policies acquire greater knowledge about the privacy practices of the SNS—potentially because it is less effortful to extract relevant information—than users who see extensive policies. One hint that participants require less cognitive effort would be that they spend less time reading the short policies but spend more time extracting relevant information (i.e., reading time per word). This should in turn result in higher knowledge about the policy's content. Therefore, we propose the following hypotheses:

> Hypothesis 1 (H1): Participants who see a short privacy policy will acquire greater knowledge about the SNS's privacy practices than participants who see a long privacy policy.
>
> Hypothesis 2 (H2): Participants who see a short privacy policy will have a higher reading time per word than participants who see a long privacy policy.
>
> Hypothesis 3 (H3): The reading time per word will be positively related to knowledge about the SNS's privacy practices.

### *2.2. Subjective Privacy Perception*

The privacy process model (Dienlin, 2014) postulates that people form a perception of privacy in any situation, both online and offline, meaning that they assess and evaluate every situation in terms of its specific privacy. For instance, being in one's own four walls should lead to a different sense of privacy than being in a public place. Likewise, different privacy perceptions might also occur online, for instance because one website is evaluated to be more private than another. However, a situation's actual level of privacy and people's perception thereof can greatly diverge (Dienlin, 2014), creating a mismatch between actual privacy levels and people's beliefs about how private the situation is (Trepte & Reinecke, 2011). This difficulty in evaluating one's current privacy level seems to be even higher in online situations than offline (Teutsch, Masur, & Trepte, 2018). Apparently, people regularly perceive privacy to be greater than it actually is. As a prominent example of this, Facebook users tend to feel "private" when they are interacting with friends, but forget that the communication is accessible to a larger audience (Vitak, 2012) and to Facebook itself.

To date, studies on how people's perception of online privacy is formed or how it can be conceptualized are scarce. Scholars have primarily focused on concepts such as privacy concerns, attitudes or intentions (e.g., Dienlin & Trepte, 2015), while research on individuals' subjective perception of the privacy level in a specific situation seems to be lacking. While privacy concerns focus on one's negative emotional attitude (Dienlin & Trepte, 2015) towards potential negative effects on one's privacy, the perception of privacy captures one's assessment of the current degree of privacy with a view to a specific application or situation. Classical privacy theories argued that privacy is about freedom and control over the decision of when and to whom to disclose (Altman, 1975; Westin, 1967). This implies that the subjective perception of a given privacy level might involve a sense of control. However, classical theories do not explicitly explain how individuals form a perception of current privacy. Focusing on this issue, a recent qualitative study by Teutsch et al. (2018) found that participants' subjective perception of (online) privacy depends on trust towards the recipient of information and the perception of control over personal information. In the present study, these findings are taken as the basis from which to conceptualize participants' subjective privacy perception. Consequently, perceived privacy is considered as the experience, sense, and evaluation of one's current level of privacy, accompanied by trust towards the information recipient and a perception of control over information. Additionally, we believe that a perception of online privacy includes the perception of how well the information recipient protects personal data.

A realistic perception of online privacy in a given situation should depend on knowledge about the actual level of privacy that is present in that situation (Teutsch et al., 2018). Situational knowledge can either be based on general privacy literacy (e.g., knowledge about how IT processes work) or on being informed about the specific situation (e.g., by reading a website's privacy policy). In the present study, we aim to investigate situational knowledge which is gained by reading the SNS's privacy policy. Following Teutsch et al. (2018), we argue that the more privacy knowledge participants possess, the more accurate their subjective privacy perception will be (i.e., the privacy perception matches the actual privacy level). By varying the actual level of privacy of the SNS, we examine how this association is affected when the SNS is described either as privacy-intrusive or as privacy-friendly:

> Hypothesis 4a (H4a): Higher knowledge about the privacy-intrusive practices will lead to a reduced perception of privacy.

> Hypothesis 4b (H4b): Higher knowledge about the privacy-friendly practices will lead to an increased perception of privacy.

### 2.3. Privacy Calculus

According to the privacy process model (Dienlin, 2014), people's situational privacy perception directly affects their self-disclosure behavior. In privacy research, however, one approach that has gained a great deal of attention—the privacy calculus (Culnan & Armstrong, 1999; Dinev & Hart, 2006)—assumes that self-disclosure behavior is the result of a cost-benefit analysis. Essentially, according to the privacy calculus, before disclosing information, people weigh privacy costs and disclosure benefits. If users associate higher benefits than costs with information revelation, they are likely to disclose personal data. If the perception of costs outweighs the perception of benefits, self-disclosure is reduced or unlikely. Several studies have found empirical support for the impact of privacy costs and benefits on self-disclosure intentions or technology adoption in a variety of different settings and contexts (e.g., Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova, Kolesnikova, & Guenther, 2009; Princi & Krämer, 2020). These studies examined various kinds of anticipated privacy costs, among them privacy concerns (e.g., Dienlin & Metzger, 2016) or privacy risk beliefs (e.g., Bol et al., 2018). In the present study, participants' assessment of the likelihood of experiencing certain privacy risks will be taken as a measure for privacy costs. This is because reading about a website's privacy practices should primarily impact one's evaluation of how likely certain privacy threats are to occur, and not, for instance, how severe privacy breaches would be.

One point of criticism regarding previous privacy calculus studies is that most did not capture the situational diversity of different disclosure decisions, and instead assessed an accumulated picture of multiple disclosure situations (Masur, 2018). Masur (2018, p. 136) defines a situation as "the entirety of circumstances that affect the behavior of a person at a given time." These circumstances are described as various internal (e.g., goals) and external factors (e.g., walls). Consequently, even visiting the same website at different points in time would result in different situations, since goals or perceptions (or sometimes also external factors like the design of the website) would change. Therefore, the anticipation of privacy costs and disclosure benefits should depend on the given situation or the perception of the circumstances of the situation (e.g., the level of given privacy). This implies that people's subjective experience of the situation's level of privacy should be related to their perception of privacy costs and benefits. In the present study, we assume that participants' assessment of the SNS's privacy level will affect the perception of privacy risk likelihood and the anticipation of benefits of using the SNS. The more one believes a situation to be private, the lower one's assessment of privacy risk likelihood should be. It might also be the case that anticipated benefits are evaluated as even more positive when one perceives a high level of given privacy. However, as we are not aware of any studies that investigated similar issues, these assumptions will be formulated as research questions:

> Research Question 1 (RQ1): Will participants' perception of privacy be negatively related to their perception of privacy risk likelihood?

> Research Question 2 (RQ2): Will participants' perception of privacy be positively related to the anticipated benefits of using the SNS?

Finally, we assume that participants' self-disclosure behavior will be in line with the assumptions of the privacy calculus (Culnan & Armstrong, 1999). To date, the privacy calculus has primarily been investigated in terms of behavioral intentions, and not the actual disclosure behaviors of individuals. A recent study, however, found that persons who had privacy concerns disclosed less information on an online discussion platform, whereas those who perceived disclosure to be beneficial actually disclosed more (Dienlin, Bräunlich, & Trepte, 2019). Hence, we also assume that the privacy calculus notions will hold with respect to actual behavior. This means that participants who perceive benefits from using the SNS should disclose more personal information, whereas those who perceive a high likelihood of experiencing privacy risks should disclose less personal information:

> Hypothesis 5 (H5): The perceived likelihood of privacy risks will be negatively related to the amount of disclosed information.

> Hypothesis 6 (H6): The anticipated benefits of using the SNS will be positively related to the amount of disclosed information.

To provide an overview over the hypothesized relations, we integrated all hypotheses and research questions into one hypothetical model (see Figure 1).

## 3. Method

### *3.1. Design and Privacy Policies*

The current study comprises a 2 (long vs. short privacy policy) × 2 (privacy-intrusive vs. privacy-friendly SNS) between-subjects design. In accordance with the experimental conditions, four different privacy policies were created. Basically, the short (around 335 words) and the long (around 2000 words) versions provided the same content but differed regarding the level of detail. The short versions summarized the different paragraphs of the long policies with bullet points providing the most important information. In the privacy-intrusive condition, the policies informed about some frequently used privacy practices, for instance, that the SNS automatically collects personal data, disseminates personal data to third parties, uses this data for advertising purposes, and applies user-tracking technologies. In the privacy-friendly condition, participants were told that the SNS mostly refrains from collecting too much personal data, does not disseminate or use this data, and does not apply user-tracking technologies.

### *3.2. Procedure*

Respondents were asked to create a personal account on an SNS which was described as providing users with personalized recommendations for leisure activities in their local area (i.e., events or locations) and to connect with peers. The SNS was introduced as a student network and as being developed by a local start-up company. Before participants created their personal account, one of the four privacy policies was displayed. Participants then had the option—but were not forced or explicitly asked—to read it. To get to the next page, they had to click on a button labeled 'got it.' On the next pages, participants were able to disclose various personal data (see Section 3.4.1) and to choose their preferred privacy setting. After they completed the registration process, they were forwarded to the survey.

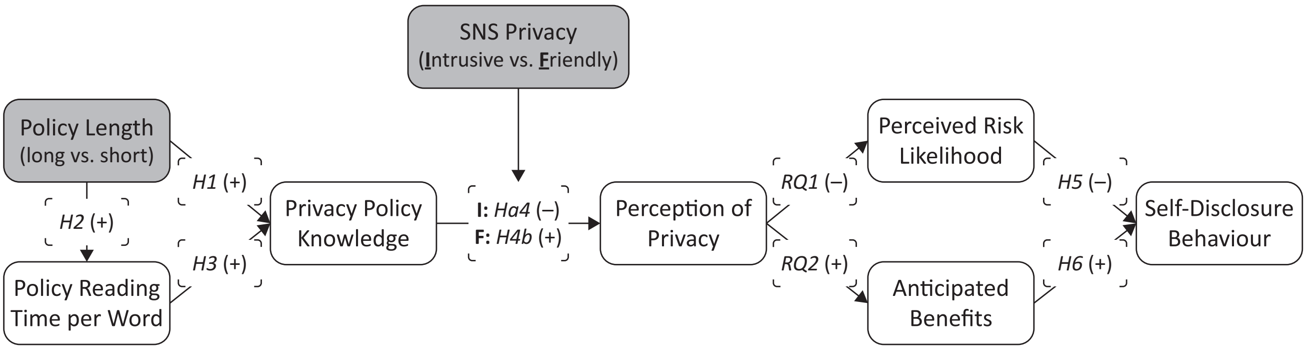


**Figure 1.** The integrative model including all hypotheses and research questions.

### *3.3. Sample*

In total, 330 persons registered on the SNS and completed the survey. Twenty persons were excluded from the analysis because they answered the questionnaires in an unrealistically fast time (less than two minutes). Another five persons had to be excluded because their account information could not be matched with the respective survey data. Hence, the final sample size consisted of $N = 305$ respondents (213 females, 90 males, 2 did not specify gender) aged 17 to 58 years ($M = 25.68$, $SD = 6.02$). As their highest educational attainment, 43.9% stated having university entrance-level qualifications and 49.05% had a university degree. The majority of participants were students (73.44%), followed by employees (20.33%). The department's ethical committee approved the design of the study. Participants were recruited via Facebook as well as websites for survey sharing (e.g., surveycircle.com) and had the chance to win monetary prizes in a lottery.

### *3.4. Measures*

Below, the measurements are listed in the same order as they appeared in the survey. All items were developed for the purpose of the study. In order to test reliability, confirmatory factor analyses for each construct were performed with SPSS Amos. As can be seen in Table 1, all scales performed well.

#### 3.4.1. Behavioral Data

Different types of behavioral data were assessed while participants interacted with the SNS. First, participants' time spent on the page showing the privacy policy was recorded and taken as a measure for reading time (in seconds). This measure was then divided by the number of words of the respective privacy policy in order to calculate the reading time per word. Self-disclosure behavior was used as dependent variable in the model, which was composed of the number of filled input fields on the SNS. Participants were able to indicate personal information (e.g., name, date of birth, gender), contact information (e.g., e-mail address, telephone number), hobbies, interests (e.g., food and drink, music preferences), information regarding their job or university, as well as religious and political views. Subsequently, respondents had the opportunity to introduce themselves to the other users of the network by writing a short text about themselves. A category that was filled with information was coded as 1 and a blank category was coded as 0. As respondents were able to leave all fields blank, the self-disclosure score ranged from 0–32. Finally, participants were asked to choose their preferred privacy setting (i.e., who can see one's information). The options were: 'only me,' 'only selected friends,' 'my friends,' 'my friends and their friends,' and 'all users.' The score was reverse-coded (1 = 'all users' and 5 = 'only me'). The privacy settings were not part of the model but appear in correlation analyses.

#### 3.4.2. Anticipated Benefits

Participants' perception of the SNS's benefits was assessed using seven items rated on a 7-point Likert scale (ranging from 1 = 'I do not agree at all' to 7 = 'I fully agree'). Items were based on the description of the SNS and consisted of a first part ('I would find it advantageous…') and a varying second part (e.g., '…if the SNS supported me in my leisure planning' or '…to experience new and interesting things using the SNS').

#### 3.4.3. Perceived Privacy

Following Teutsch et al. (2018), eight items were created to capture participants' evaluation of the situation's privacy level using a 7-point Likert scale (ranging from 1 = 'I do not agree at all' to 7 = 'I fully agree'). The scale consisted of items that assessed perceived control over information (e.g., 'The SNS leaves control over my personal data to me'), trust towards the SNS (e.g., 'The SNS is always honest with me about how my personal information is used'), as well as a general perception of privacy (e.g., 'The SNS is a private space') and privacy protection (e.g., 'The SNS protects my data appropriately').

#### 3.4.4. Privacy Policy Knowledge

Participants' knowledge of the SNS's privacy practices that were described in the privacy policies was assessed by nine true/false questions derived from the presented privacy policies. Besides the options 'true' and 'false,' participants were able to state 'I don't know' in order to avoid forcing them to choose an option, which might have led to biased results. A correct answer was coded as 1 and a false answer was coded as 0. 'I don't know' was also coded as 0. Consequently, the score ranged from 0 (only false/no answers) to 9 (only correct answers).

**Table 1.** Results of the confirmatory factor analyses with fit indices. Internal consistency (Cronbach's $\alpha$, composite reliability (MacDonald's $\Omega$), and average variance extracted) of the assessed constructs.

| | $\chi^2$ (df) | $p$ | CFI | TLI | RMSEA | SRMR | $\alpha$ | $\Omega$ | AVE |
|---|---|---|---|---|---|---|---|---|---|
| Anticipated Benefits | 33.99 (13) | .001 | .99 | .98 | .07 | .02 | .93 | .93 | .66 |
| Perceived Risk Likelihood | 1.08 (2) | .582 | 1.00 | 1.00 | $< .01$ | .01 | .83 | .83 | .54 |
| Perceived Privacy | 39.82 (19) | .003 | .99 | .98 | .06 | .02 | .93 | .93 | .62 |

### 3.4.5. Perceived Likelihood of Privacy Risks

Participants assessed the likelihood of negative consequences of using the SNS with a slide bar ranging from 0% to 100%. The seven items were based on the content of the privacy policies and consisted of a first part ('How likely do you think it is…') and a varying second part (e.g., '…that the SNS passes on your personal data to third parties' or '… of being exposed to privacy risks by using the SNS'). Three items were deleted within the confirmatory factor analyses.

## 4. Results

Data were analyzed with IBM SPSS Statistics 25 and IBM SPSS Amos 25. Table 2 shows descriptive statistics, and Table 3 displays bivariate correlations between the variables.

### *4.1. Structural Equation Model*

The hypotheses and research questions were tested within one structural equation model (SEM) with observed variables and maximum likelihood estimation. Model fit was evaluated in accordance with frequently used fit indices (Browne & Cudeck, 1993; Hu & Bentler, 1999). The model test revealed a good fit: $\chi^2$ (13) = 16.48, $p$ = .224, $\chi^2$/df = 1.27, CFI = .98, TLI = .96, RMSEA = .03 (90% CI: .00, .07), SRMR = .04. The model is shown in Figure 2. H1 expected that participants who read the short privacy policies would have increased knowledge about the SNS's privacy practices compared to participants who read the long versions. Contrary to this assumption, there was no relationship between policy length (coded as 1 = 'long' and 2 = 'short') and policy knowledge ($\beta$ = .00, $p$ = .997). In H2, we assumed that participants would have a higher reading time per word when confronted with a short privacy policy. This hypothesis was supported, as we found a positive relationship between the two variables ($\beta$ = .30, $p < .001$). The analysis of H3 found support for the assumption that a higher reading time per word positively contributes to knowledge about the SNS's privacy practices ($\beta$ = .31, $p < .001$). H4 expected a negative relation between policy knowledge and perceived privacy in the privacy-intrusive condition (H4a), and a positive relation in the privacy-friendly condition (H4b). We used a multigroup analysis to examine whether the relationship behaves equivalently in different subsamples (Kline, 2016). As the model fit of the unconstrained model was not acceptable, an additional path between privacy policy knowledge and risk likelihood had to be drawn based on the modification indices. The adjusted model showed a good data fit: $\chi^2$ (24) = 24.38, $p$ = .440, $\chi^2$/df = 1.02, CFI = 1.00,

**Table 2.** Descriptive statistics of the assessed constructs and behavioral data.

| | | Range | |
|---|---|---|---|
| | *M* (*SD*) | Actual | Potential |
| Perceived Benefits | 4.91 (1.41) | 1–7 | 1–7 |
| Perceived Risk Likelihood | 6.06 (2.02) | 1–11 | 1–11 |
| Perceived Privacy | 4.03 (1.27) | 1–7 | 1–7 |
| Privacy Policy Knowledge | 2.96 (2.34) | 0–8 | 0–9 |
| Policy Reading Time (seconds) | 33.32 (68.13) | 1–532 | ∞ |
| Reading Time per Word | 0.05 (0.08) | .00–.63 | ∞ |
| Self-Disclosure (filled fields) | 14.93 (6.28) | 0–24 | 0–32 |
| Privacy Setting | 3.62 (1.52) | 1–5 | 1–5 |

Notes: Risk likelihood was assessed with a percentage scale, meaning that a value of 1 equals 0%, 6 equals 50% and 11 equals 100%. Privacy setting was reverse-coded with 1 = 'public' and 5 = 'private.'

**Table 3.** Bivariate correlations between all assessed constructs and behavioral data.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 Perceived Benefits | — | | | | | | | |
| 2 Perceived Risk Likelihood | −.12 * | — | | | | | | |
| 3 Perceived Privacy | .24 *** | −.45 *** | — | | | | | |
| Privacy Policy Knowledge | | | | | | | | |
| 4 Privacy-Intrusive Website (*n* = 148) | .02 | .39 *** | −.29 *** | — | | | | |
| 5 Privacy-Friendly Website (*n* = 157) | .01 | −.33 *** | .41 *** | — | — | | | |
| 6 Policy Reading Time (seconds) | .00 | −.12 * | .11 | .26 *** | .32 *** | — | | |
| 7 Reading Time per Word | .06 | −.06 | .05 | .28 *** | .37 *** | .62 *** | — | |
| 8 Self-Disclosure (answered fields) | .18 ** | −.07 | .03 | .02 | .04 | .04 | −.03 | — |
| 9 Privacy Setting | −.16 ** | .05 | .02 | −.20 * | −.01 | −.09 | −.10 | −.25 *** |

Note: * $p < .05$, ** $p < .01$, *** $p < .001$.

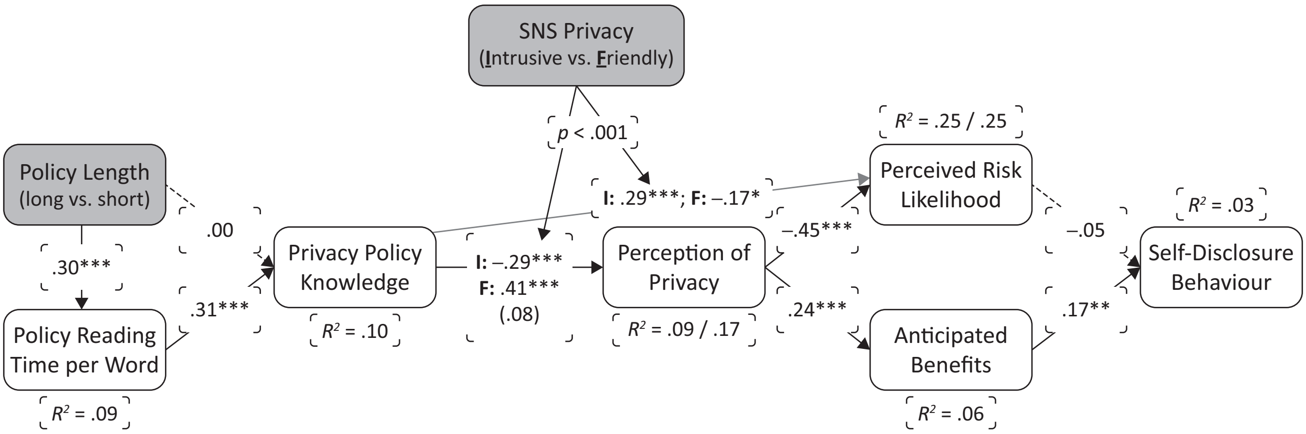


**Figure 2.** SEM with observed variables. Notes: The gray line was added in the multigroup analysis based on modification indices. Numbers display standardized regression coefficients ($\beta$). When two $R^2$ values are displayed, these are part of the multigroup analyses (privacy-intrusive condition first, privacy-friendly condition second). Numbers in brackets shows the effect size without group effects. Dashed lines indicate non-significant paths. $^*p < .05$, $^{**}p < .01$, $^{***}p < .001$.

TLI = 1.00, RMSEA = .01 (90% CI: .00, .05), SRMR = .06. The multigroup analysis revealed that the paths differed significantly between the two conditions ($\Delta(\chi^2) = 58.61$, $\Delta(p) < .001$).

In accordance with H4, the multigroup analysis revealed that higher knowledge about the privacy practices in the privacy-intrusive condition led to a decreased perception of privacy ($\beta = -.29$, $p < .001$), whereas higher knowledge in the privacy-friendly condition positively affected privacy perception ($\beta = .41$, $p < .001$). The subsequently added path between knowledge and perceived risk likelihood revealed a positive relation in the privacy-intrusive condition ($\beta = .29$, $p < .001$), and a negative relation in the privacy-friendly condition ($\beta = -.17$, $p = .026$). This finding implies that knowledge about the content of privacy policies can lead to a more accurate assessment of the likelihood of privacy risks. Moving onward to the research questions, testing RQ1 revealed that participants' evaluation of the current degree of privacy was negatively related to their assessment of privacy risk likelihood ($\beta = -.45$, $p < .001$). Concerning RQ2, there was a positive relation between privacy perception and the anticipation of self-disclosure benefits ($\beta = .24$, $p < .001$). Thus, the results are in line with the assumptions of both research questions. No support was found for H5, since the perceived likelihood of privacy risks did not show a significant negative relation to the amount of information disclosed on the SNS ($\beta = -.05$, $p = .374$). Finally, the perception of benefits was significantly positively related to the amount of disclosed data, thus supporting H6 ($\beta = .17$, $p = .003$).

### *4.2. Additional Analysis*

To shed more light on the finding that the reading time per word was higher in the short policy condition, we conducted a MANOVA with total reading time and with reading time per word. The results ($F$(1, 303) = 7.62, $p = .006$, $\eta^2 = .025$) showed that the actual reading time was significantly higher in the long policy condition ($M = 44.01$, $SD = 90.01$) compared to the short policy condition ($M = 22.71$, $SD = 30.83$). For reading time per word, the results of the MANOVA ($F$(1, 303) = 30.20, $p < .001$, $\eta^2 = .091$) revealed a lower value in the long condition ($M = .02$, $SD = .05$) in comparison to the short condition ($M = .07$, $SD = .09$). Hence, although the average reading time in the long condition was about twice as high as in the short condition, the reading time per word was more than three times higher in the short condition compared to the long condition. This emphasizes that the short text was more successful in delivering knowledge than the long text, due to the fact that a more effective information extraction was possible.

## 5. Discussion and Conclusion

The current study pursued two major aims. The first aim was to investigate whether shorter privacy policies can be more beneficial to inform SNS users about potential privacy costs compared to long versions. The second aim was to test assumptions regarding users' privacy decisions stemming from two approaches (i.e., the privacy process model and the privacy calculus) within one integrative model. The results provide insights into the relevance of privacy policy design for individual privacy information acquisition, the importance of knowledge about actual privacy levels, and situational factors underlying self-disclosure. In terms of practical implications, policy makers and politicians may consider our findings for the design of privacy policies and the development of guidelines for such policies.

### *5.1. Privacy Policy Length*

The first three hypotheses focused on whether shorter privacy policies would be more beneficial in informing users about a website's privacy practices than longer versions, and whether participants would have to expend less effort on reading the short versions. Since survey data (e.g., European Commission, 2019) revealed that few users read privacy policies, we argued that for most people, reading privacy policies is associated with (cognitive) effort. Hence, people might be more motivated to read condensed versions due to the lower anticipated cognitive and time effort (cf. Lang, 2017). In the present study, participants were given the option of whether to read the privacy policy of the SNS on which they would subsequently create an account. Although the results did not reveal a direct effect of policy length on knowledge about the content of the policy, we nevertheless found that short privacy policies can indeed be more advantageous than long ones: First, participants who saw a short policy had a higher reading time per word, meaning that they chose to spend more time on understanding the given text. Second, the reading time per word was then positively related to knowledge about the policy's content. This demonstrates that shorter privacy policies indirectly contribute to higher knowledge about their contents compared to the normally applied long versions. However, this effect only exists among persons who actually expend some effort on reading the policies. The effort to extract information from the text, however, was found to be significantly reduced for the short privacy policy, because participants were able to read the text more carefully and understand the text in less time compared to participants who saw the long policy. According to the assumptions of Lang (2017), these findings indicate that people were more willing to engage in reading the shorter policy. Taken together, the results demonstrate that participants were able to absorb more information from the shorter policies and probably had a higher motivation to do so. The GDPR prescribes that policies should be written in comprehensible language to enhance transparency. However, policies of immense length oppose the goal of informing users. Hence, the present findings could be used by politicians to obligate companies to truly inform users by providing short, comprehensible privacy policies instead of allowing companies to provide long and complicated policies which primarily serve the purpose of avoiding lawsuits. While it might be argued that shortening texts brings about a loss of information, we believe that Internet users do not need to be provided with the abundance of information that is written in standard privacy policies at the time when they normally have to give their consent to data processing. Our study findings show that for individuals who wish to register on websites, the provision of less information would be beneficial for informing them about the main privacy practices. For those who wish for more detailed information, the long policies could still be available in addition to the short ones. Nonetheless, the present findings also revealed that shortening privacy policies is not a panacea in itself; the responsibility to inform oneself and protect one's privacy still lies with the user. However, users seem to be more motivated to engage in information-gathering when the privacy policy is short. It must be noted that participants' knowledge of the policies' content was rather low. Thus, providing short informative privacy policies might be a first step toward greater privacy policy knowledge and informed privacy decisions of social media users. However, there is still a great need for research on how to create more transparency to inform users and how to automatically protect users' privacy (e.g., using privacy-by-design approaches or real-time support provided by software). It is becoming increasingly apparent that users might benefit from support in their privacy decisions, given that they are not always able to balance their needs for self-disclosure and privacy protection on their own (Krämer & Schäwel, 2020).

### *5.2. Privacy Decision-Making*

With H4 to H6 and RQ1 and RQ2, we sought to examine how different constructs relevant for online privacy decisions are related. The integrative model was based on parts of the privacy process model (Dienlin, 2014), which assumes that individuals form a privacy perception in any situation, and the privacy calculus (Culnan & Armstrong, 1999), which states that self-disclosure decisions are the result of a cost-benefit analysis. We argued that the subjective perception of the situation's privacy should be based on knowledge about the privacy policy's content (H4). The results supported the assumptions that more knowledge led to a lower perception of privacy in the privacy-intrusive condition and to a higher perception of privacy in the privacy-friendly condition. This finding demonstrates that factual knowledge about the degree of privacy in a situation can advantageously contribute to one's feeling of privacy by resolving potential mismatches between the objective situation and the subjective perception (cf. Trepte & Reinecke, 2011), supporting previous assumptions (Dienlin, 2014; Teutsch et al., 2018). In turn, people who lack knowledge may more easily misperceive actual privacy levels and become victims of privacy breaches, as they might share inappropriate (amounts of) data due to a false perception of situational privacy. Previous research has found that general privacy knowledge (i.e., privacy literacy) can positively contribute to more protective privacy behaviors (e.g., Bartsch & Dienlin, 2016). Together with the results of the present study, it seems that both general knowledge and situational knowledge are important for online privacy perception and behavior. Future studies could also pursue the questions of whether privacy literacy affects the situational feeling of privacy, or how general and situational knowledge are related. It must be noted that the amount of explained variance in privacy perception was rather low in the current study, indicating that situational knowledge is only one of several factors that influence the evaluation of online privacy levels. Without appropriate knowledge, people might rely on heuristics (e.g., triggered by the design of a website) or general feelings or beliefs (e.g., thinking that online privacy is always low or high). Besides our hypotheses, the analysis revealed a direct effect of policy knowledge on the assessment of privacy risk likelihood. In the privacy-intrusive condition, the perceived risk likelihood increased with higher knowledge, whereas in the privacy-friendly condition, knowledge reduced the perceived risk likelihood. Although not part of our hypotheses, it is plausible that people with higher knowledge about a website's privacy practices are better able to estimate the likelihood of potential negative consequences of website usage.

Next, we investigated whether the situational perception of privacy affects the perceived likelihood of privacy risks (RQ1) and the anticipation of benefits of using the SNS (RQ2). The results revealed that the perception of online privacy was indeed related to both risk likelihood appraisal and benefit perception. The more private the situation was perceived to be, the lower respondents assessed the likelihood of negative consequences to be, and the higher they rated the benefits of using the SNS. These results support the assumptions of Masur (2018), who argued that the assessment of privacy costs and disclosure benefits differs for each situation. The present findings show that the perception of privacy risk likelihood and disclosure benefits can vary based on the evaluation of given privacy levels, implying that the weighing of costs and benefits is not stable but rather varies across different situations. While the negative relation between participants' perception of privacy and their assessment of privacy costs is more intuitive (private situations should by definition entail a reduced likelihood of privacy risks), the positive link between privacy perception and benefit perception is an interesting finding. It seems that participants appreciated the privacy-preserving SNS, which led to an increased perception of benefits. Hence, websites that respect user privacy could have an advantage over websites that do not, because people might turn towards the privacy-preserving ones. However, this interpretation is only speculative, and no causal implications can be drawn. Therefore, future studies might consider the role of Internet users' perception of present privacy levels and the antecedents and outcomes thereof.

Finally, hypotheses H5 and H6 focused on the privacy calculus, assuming that participants would disclose less information if they considered privacy risks as likely to happen and would disclose more information if they perceived disclosure to be beneficial. However, only the perception of benefits was significantly positively associated with the amount of disclosed data. Participants who thought that privacy risks were likely did not disclose significantly less personal information. These results are contrary to the basic assumption of the privacy calculus and contradict the findings of a recent study that also collected behavioral data (Dienlin et al., 2019). Although plenty of studies have found support for the basic assumption of the privacy calculus (e.g., Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova et al., 2009; Princi & Krämer, 2020), the approach is not without criticism (Knijnenburg et al., 2017). The vast majority of privacy calculus studies focused on intentions rather than on behavioral data (with the exception of the study by Dienlin et al., 2019). Hence, it may be that the privacy calculus holds in hypothetical decisions but not in concrete disclosure situations. However, we propose some alternative explanations. First, even the positive effect of benefit perception on self-disclosure was comparatively small and the proportion of explained variance in self-disclosure was very low. This implies that the disclosure decision was primarily based on factors other than the perception of benefits, possibly because participants were aware of the artificial experimental situation. This might also be the reason why privacy risk perception did not have any effect on participants' self-disclosure behavior. Second, we did not collect survey data of those persons who decided not to register on the SNS. Thus, it might be the case that the persons who registered were primarily those for whom privacy risks are less important. Third, we are unable to make any statements about whether participants actually weighed risks and benefits, although this is the basic assumption of the privacy calculus. It may be that many participants balanced costs against benefits but came to the conclusion that the benefits were worth the risks (cf. Trepte et al., 2015). Hence, future studies should collect behavioral data on the privacy calculus and investigate different privacy situations in order to better understand the dynamics underlying privacy decision-making.

### *5.3. Limitations*

Some limitations of the present study should be mentioned. For most paths in the model, it is not possible to make causal statements. Moreover, participants did not freely decide to register on the SNS, but were told to do so as part of the study. This created an artificial situation and might have distorted some behavioral data on the SNS. A further limitation pertains to the sample, which mainly consisted of females, students and highly educated persons, and is thus not representative of the general population. Moreover, the items concerning privacy risk likelihood and SNS benefits contained only a limited number of potential negative and positive consequences. It is conceivable that participants anticipated further risks or benefits of using the SNS that were not captured. Since only those who registered for the SNS were also able to participate in the study, future studies should also allow participants to not disclose personal data while still capturing their response behavior. This method could prevent distorted samples and uncover interesting findings. In addition to this point, a further limitation concerns the recruitment, which partially occurred via Facebook and may thus also have distorted the sample. Another issue concerns the measurement of self-disclosure: Some participants disclosed more detailed information than others (e.g., exact date of birth vs. year of birth) and some disclosed false information (real name vs. nickname). However, we did not consider these differences in the analysis but used a simplified self-disclosure score focusing on the amount of disclosure. This approach, however, might be an oversimplification of behavior which might have distorted results in some respects. Finally, with respect to the external validity of the study, since participants disclosed data in one specific SNS, it is unclear whether the same relationships would be found in different situations.

### *5.4. Conclusions*

The present study contributes to our understanding of online privacy in two ways: First, the findings indicate that shorter privacy policies can increase users' reading accuracy (while reading time and probably cognitive effort are decreased) and knowledge. This implies that people might be more willing to read shorter privacy policies about a website's potential privacy costs, which in turn enhances their knowledge. Whereas the GDPR prescribes that policies must be written in an understandable language style, legislators could also think about prescribing shorter versions of privacy policies (possibly in addition to the traditional long ones) since this can support users in terms of information acquisition. Second, an integrative model was tested that was composed of parts of two different approaches and contained factors relevant for online privacy decision-making. Several interesting findings emerged. Factual knowledge about the content of the privacy policies seems to be an important factor for the evaluation of one's current online privacy level as well as the assessment of privacy risk likelihood. The more participants knew about actual levels of privacy, the more realistic their feeling of privacy was. The subjective perception of privacy led to different perceptions of privacy costs and self-disclosure benefits. This suggests that situational perceptions can impact and distort the weights of anticipated negative and positive consequences of disclosure. Finally, participants disclosed more personal information when they perceived higher benefits of using the SNS. Given the importance of factual privacy knowledge, policy makers should seek ways to increase Internet users' situational privacy knowledge, as this is related to other factors underlying privacy decisions. According to the findings of the present study, shortened privacy policies represent one such way to better inform website users about situational privacy issues.

## Acknowledgments

This work has been funded by the Federal Ministry for Education and Research of Germany (No. 16KIS0743). We acknowledge support by the Open Access Publication Fund of the University of Duisburg-Essen.

## Conflict of Interests

The authors declare no conflict of interests.

## References

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

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

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., . . . de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. *Sociological Methods & Research*, *21*(2), 136–136. https://doi.org/10.1177%2F0049124192021002005

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J.-M. Mönig (Eds.), *Medien und Privatheit* [Media and privacy] (pp. 105–122). Passau: Stutz.

Dienlin, T., Bräunlich, K., & Trepte, S. (2019). *How do like and dislike buttons affect communication? A privacy calculus approach to understanding self-disclosure online in a one-week field experiment*. Paper presented at the 69th Annual Conference of the ICA, Washington, DC, USA.

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

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

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

European Commission. (2019). *Special Eurobarometer 487a: The general data protection regulation*. Brussels: European Commission. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation*

*Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). New York, NY: The Guilford Press.

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). Death to the privacy calculus? *SSRN Electronic Journal*. Retrieved from https://doi.org/10.2139/ssrn.2923806

Krämer, N. C., & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, *31*, 67–71. https://doi.org/10.1016/j.copsyc.2019.08.003

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). "It won't happen to me!": Self-disclosure in online social networks. In *Proceedings of the 15th Americas Conference on Information Systems* (pp. 1–9). Atlanta, GA: AIS/ICIS. Retrieved from http://aisel.aisnet.org/amcis2009/343

Lang, A. (2000). The limited capacity model of mediated message processing. *Journal of Communication*, *50*(1), 46–70. https://doi.org/10.1111/j.1460-2466.2000.tb02833.x

Lang, A. (2017). Limited capacity model of motivated mediated message processing (LC4MP). In P. Rössler, C. A. Hoffner, & L. van Zoonen (Eds.), *The international encyclopedia of media effects* (pp. 1–9). Hoboken, NJ: John Wiley & Sons. https://doi.org/10.1002/9781118783764.wbieme0077

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

Princi, E., & Krämer, N. (2020). I spy with my little sensor eye: Effect of data-tracking and convenience on the intention to use smart technology. In *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 1391–1400). Maui, HI: University of Hawaii, Manoa. https://doi.org/10.24251/HICSS.2020.171

Teutsch, D., Masur, P. K., & Trepte, S. (2018). Privacy in mediated and nonmediated interpersonal communication: How subjective concepts and situational perceptions influence behaviors. *Social Media + Society*, *4*(2), 2056305118767134. https://doi.org/10.1177%2F2056305118767134

Trepte, S., & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47–60). Heidelberg: Springer.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Heidelberg: Springer. http://dx.doi.org/10.1007/978-94-017-9385-8

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470. https://doi.org/10.1080/08838151.2012.732140

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

## About the Authors

**Yannic Meier** is a PhD Candidate and Research Associate in the Team Social Psychology: Media and Communication at the University of Duisburg-Essen, Germany. He is a Member of the research project 'Forum Privacy' that works on an interdisciplinary understanding of the role of privacy. In his dissertation, he studies mechanisms of online privacy decision-making and supportive means for online privacy protection. His research interests include online privacy, online self-disclosure, and entertainment research.

**Johanna Schäwel** is a Postdoctoral Researcher in the field of media psychology and communication at the University of Hohenheim in Germany. She finished her PhD in 2018 at the University of Duisburg-Essen, Germany, in the field of social psychology and media psychology. In her dissertation, she focused on online privacy protection and psychological factors that influence the acceptance of technical privacy support. Her research focuses on online privacy, self-disclosure and self-presentation on social networking sites, and persuasive processes of communication.

**Nicole C. Krämer** is Full Professor of Social Psychology, Media and Communication at the University of Duisburg-Essen, Germany. She completed her PhD in Psychology at the University of Cologne, Germany, in 2001, and received the *venia legendi* for psychology in 2006. Dr. Krämer's research focuses on social psychological aspects of human-machine-interaction (social effects of robots and virtual agents) and computer-mediated-communication. She investigates processes of information selection, opinion building, and relationship maintenance of people communicating via Internet, especially via social media.

Media and Communication (ISSN: 2183–2439)
2020, Volume 8, Issue 2, Pages 302–313
DOI: 10.17645/mac.v8i2.2850

Article

# Polish Privacy Media Discourse: Privacy as Imposed Policies

Łukasz Wojtkowski *, Barbara Brodzińska-Mirowska and Aleksandra Seklecka

Department of Communication, Media and Journalism, Nicolaus Copernicus University, 87–100 Toruń, Poland;
E-Mails: wojtkowski@umk.pl (Ł.W.), brodzinska@umk.pl (B.B.-M.), seklecka@umk.pl (A.S.)

* Corresponding author

Submitted: 29 January 2020 | Accepted: 7 May 2020 | Published: 23 June 2020

**Abstract**

In this article we look at the Polish media discourse on privacy. In the analysis, we draw on theoretical approaches that understand privacy as having four dimensions: relational, participatory, contextual, and technological. Moreover, we seek whether a specific norm of data-related privacy could be defined/redefined within the discourse. Considering the post-communist past that shapes a specific approach to surveillance and the general polarisation of polish media discourse, one would expect the key role of privacy issues in the public sphere. Thus, applying a critical discourse studies analysis, the aim was to capture the character of the so far under-researched privacy in Polish media discourse. We study what types of institutional agents are mentioned as creating privacy policies and what dimensions of privacy they tackle. Moreover, we also try to capture whether the institutional position offers a specific normative understanding of privacy and whether this norm is citizen/user-oriented. The results of the study indicate that: both the media discourse and the normative content of privacy policies are dominated by legal aspects concerned with the issues resulting from EU regulations (i.e., General Data Protection Regulation); privacy policies are institutionally dispersed and monopolised by journalists and experts instead of state officials or politicians; and there is only limited evidence of a discursive frame of a citizen-oriented norm of how to protect data-related privacy.

**Keywords**

critical discourse studies; General Data Protection Regulation; media discourse; Poland; privacy; privacy-invasive politics

**Issue**

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

## 1. Introduction

The implementation of the General Data Protection Regulation (GDPR) in mid-2018 triggered a Polish media discourse on privacy and animated the first Polish discussion on data protection. The Polish case can be considered as intriguing given its unique historical and contemporary political contexts. Post-communist countries have a sole approach to some privacy issues, for example surveillance. They are also more likely to show general anxiety, which corresponds to increased surveillance concerns (Svenonius & Björklund, 2018). Given this, it might be expected that the issue of privacy would be a particularly salient one Poland, but it was mainly neglected for the last three decades. At the same time, Polish society faces the development of privacy-invasive institutional practices and their consequences for the public. Contemporary political changes in Poland after the electoral victory of conservative and anti-European parties lead to introduction of new surveillance (i.e., the Pegasus surveillance system). Moreover, development of political microtargeting based on users' data resulted in advanced usage of disinformation tools in political campaigns in Poland (Gorwa, 2017). Although the development of privacy-invasive politics and technologies in Poland was tackled in terms of surveillance (Centrum Badania Opinii Społecznej, 2016; Sojka, 2013; Szumańska, Klicki, Niklas, Szymielewicz, & Walkowiak, 2016) or online security (Centrum Badania Opinii Społecznej, 2018) there is limited, up-to-date, and rigorous research output that captures these issues.

On the academic level, there is no comprehensive research on the nature of Polish media discourses on privacy. Only partially, privacy and surveillance were analysed by Möller and Nowak (2018b) in terms of privacy-oriented media practices of civil society agents, by Ptaszek (2018) who studied attitudes and knowledge on surveillance and privacy among adolescents, or by Svenonius and Björklund (2018) who comparatively explored the attitudes to surveillance in post-communist societies. However, privacy-related issues are under-researched when it comes to discourse studies. To fill this gap, this article aims to analyse the character of contemporary privacy media discourse in Poland. We study what privacy dimensions are tackled by particular types of institutional agents promoting privacy policies in the media discourse. Moreover, we try to capture whether the discourse reflects a specific normative understanding of privacy and whether this norm is citizen/user-oriented. By that, we expect to see whether a specific privacy dimensions and agents framed in the discourse enhance normatively citizens and users or, on the contrary, reinforces inequality and imbalance where state actors and tech companies build the privacy-invasive norm. To do so, we have designed a research framework that follows Nissenbaum's (2010) idea of contextual integrity that understands privacy as being contextual and having a normative element. Based on this, we attempt to ascertain whether norms of data-related privacy can be (re)defined in the discourse. Moreover, we implement Möller and Nowak (2018a, 2018b) take in which theoretical approaches to privacy are considered as four dimensional: Contextual, relational, participatory, and technological.

## 2. Theoretical Framework

Our theoretical approach uses the discursive analysis to track the character of Polish media discourse on privacy. We understand discourse as a form of communicative social practice. In other words, "texts, as forms of interaction, are seen as discursive practices, and these discursive practices are also social practices" (Bennett, 2018). It means that the discourse reaches above the level of language. It is rather a "a two-way relationship between a particular discursive event and the situation(s), institution(s) and social structure(s), which frame it: the discursive event is shaped by them, but it also shapes them" (Unger, Wodak, & KhosraviNik, 2016, p. 907). In the context of this article, this means that the social institutions 'think' and 'act' according to how they 'speak' about it. Hence, tracking the privacy dimensions in the media discourse allows for analysis of the understandings of privacy in relation to institutional actors putting them forward available in the Polish public debate.

In general, the Polish political discourse can be captured with three most distinctive features. The first one is polarisation, where the discourse re-creates political divisions and frames the oppositional camps (Balczyńska-Kosman, 2013) and ideological conflicts (Czyżewski, Kowalski, & Piotrowski, 2010). The second concerns negativity and emotionality, where institutional actors frame particular political issues in terms of negative labelling of the opponents (Balczyńska-Kosman, 2013). The third is the media-orientation, where media shape the political discourse due to specific priming and framing (Balczyńska-Kosman, 2013). Thus, the question rises if the discourse on privacy also follows such characteristic? Especially when we compare it to Germany where the issues of privacy are addressed in terms of criticizing the current level of privacy and the need of enhancing it (cf. von Pape, Trepte, & Mothes, 2017) or normalization of surveillance technology (Meissner & von Nordheim, 2018).

As a starting point in seeking traces of privacy in the discourse, we apply the Nissenbaum's idea of contextual integrity (2010) and multi-dimensional composition of privacy proposed by Möller and Nowak (2018a). Thus, we use the approach where privacy is characterised by five dimensions: Contextual, normative, relational, participatory, and technological.

Firstly, privacy is contextual and as such must be situated and researched in specific contexts. Nissenbaum introduces the notion of contextual integrity that:

> Provides a rigorous, substantive account of factors determining when people will perceive new information technologies and systems as threats to privacy; it not only predicts how people will react to such systems but also formulates an approach to evaluating these systems and prescribing legitimate responses to them. (Nissenbaum, 2010, p. 2)

Thus, privacy depends on and constitutes social norms, resources, rules, and cultural arrangements that may substantially differ from one society to another. For example, when considering technology as a threat to privacy, this is contextual and has to be perceived whilst taking multiple variables into account (including cultural, historical, and even geographical). Yet, according to Nissenbaum (2010, p. 11), the framework of contextual integrity fits "to model peoples' reactions to troubling technology-based systems and practices as well as to formulate normative guidelines for policy, action, and design." Thus, concerning Polish historical and contemporary privacy-invasive politics, the way in which discourse on privacy is framed may shed more light on how the particular contexts effect or model the privacy policy addressed by institutions.

Secondly, privacy is normative. Thus, a normative approach to privacy attempts to capture whether a specific norm of data-related privacy is present within the media discourse. Drilling down, a more specific question is whether this norm is citizen-oriented or not. Both Möller and Nowak's (2018a), and Nissenbaum's (2010) frameworks are practice-oriented and dwell on the idea that users are able to respond to the surveillance using media technologies. Or, to fine tune it slightly, how people should take care of their privacy and data protection while they use communication technologies. This is especially germane to the Polish media discourse case, where data protection and privacy are relatively new phenomena. Indeed, the GDPR's introduction launched the first major national discussion on privacy, not only by prescribing some legal norms but also by exposing the category of 'privacy' in the discourse, making it visible and discussed in society.

Möller and Nowak (2018a), who draw on Nissenbaum's approach, aside from contextual privacy, list three other dimensions: relational, participatory, and technological. Thus, thirdly, relational privacy concerns the relationship between people, the information they produce and the third parties that manage the information. Understood in such a way, privacy depends on the place of the individual (or institution) in relation to the level of privacy and openness one wants to preserve within communication processes in society (cf. Westin, 2015). Concerning the media discourse, this dimension allows observing how the discourse manifests the relations between society shaped by post-communist experiences and the state that conducts a privacy-invasive politics. The relational dimension regarding privacy in the Polish discourse is also important since Poles believe that data sharing is non-alternative and data protection is becoming a very important issue for citizens (European Commission, 2015). Thus, regarding the state's politics, one would expect the media discourse to refrain citizen-oriented relation in order to protect people's privacy.

Fourthly, privacy is participatory, which means that the actual privacy practices presume the active participation of individuals in the process of setting the privacy. This dimension, on the one hand, allows for tracing the media discourse in Poland in terms of privacy as a bottom-up perspective when it is actively implemented in the everyday media practices of users (Kubitschko, 2018). As the studies prove, Polish users' privacy practices are following the idea of "acting on media" in terms of surveillance (Möller & Nowak, 2018b). On the other hand, participatory dimension considers also the advocacy of organisations that participate actively in promoting privacy (Bennett, 2008). The search for a manifestation of the participatory dimension in the privacy discourse in Poland can be linked to the activity of privacy advocacy organizations as Panoptykon (a countersurveillance and privacy advocacy NGO) or Zaufana Trzecia Strona (data security and privacy advocacy collective). Thus, traces of the participatory dimension in the discourse will indicate not just the specific privacy practices but also the politics of privacy that such institutions propose.

The last dimension is a technological one. The privacy-oriented practices of individuals and groups strongly rely on communication technologies and data protection. Digital technology and social media companies that offer the unlimited space for interactions are the most powerful data-harvesters. At the same time, users' access to their personal data is efficiently limited. Eventually, a communication market evolves towards an imbalanced struggle between centralized privately-controlled data flows and decentralization, i.e., giving it back to users (Möller & von Rimscha, 2017). Thus, to some extent, the technological dimension of privacy can be understood as a common discursive thread that can run through the other dimensions.

Such theoretical framework allows us to state the main research question: What is the character of media discourse on privacy in Poland? To answer it, we state two subordinate research questions: a) Which institutional agents construct the media discourse; and b) how privacy is framed in the media discourse? Firstly, we conceptualise the character of the institutional discourse on privacy in terms of the five aforementioned dimensions. However, the character of the media discourse may also reflect some other specific features that are illustrative for Polish discourse in general. Thus, besides of the dimensions we search for specific issues concerning media-orientation, publisher's political position and attitude towards the economy or possible discursive polarisation. Secondly, we search for institutional actors that form the media discourse on privacy. Thus, we analyse how certain dimensions are approached by social institutions and their representatives, including politicians, officials, journalists, experts, or ordinary people. Thirdly, we look at how the discursive relationship between institutions and dimensions is framed in linguistic categories.

## 3. Research Design and Methodology

To answer the research questions, we apply a critical discourse studies (CDS) approach that follows the methodological framework recommended by Unger et al. (2016, pp. 1191–1197). A crucial fact to note is that the applied CDS approach is inductive but it requires state-of-art analysis concerning existing theoretical knowledge on the particular case. Thus, the analytical procedure started with the theoretical notions on discourses of privacy and resulted in shaping the theoretical model and particular privacy-related discursive categories (see Figure 1).

Then, we executed a CDS approach in a three-stage data-based inductive analysis (Unger et al., 2016). Firstly, to have a general outlook on the shape of the discourse, we undertook desk research of privacy-oriented publications from two privacy-activist media websites and one privacy-advocacy NGO website. This totalled 133 privacy-oriented cases from January 2018 to September 2019. It allowed us to extract a list of issues related to privacy in the Polish media discourse in that particular time. As desk research indicated, Polish media discourse was dominated by certain events rather than by

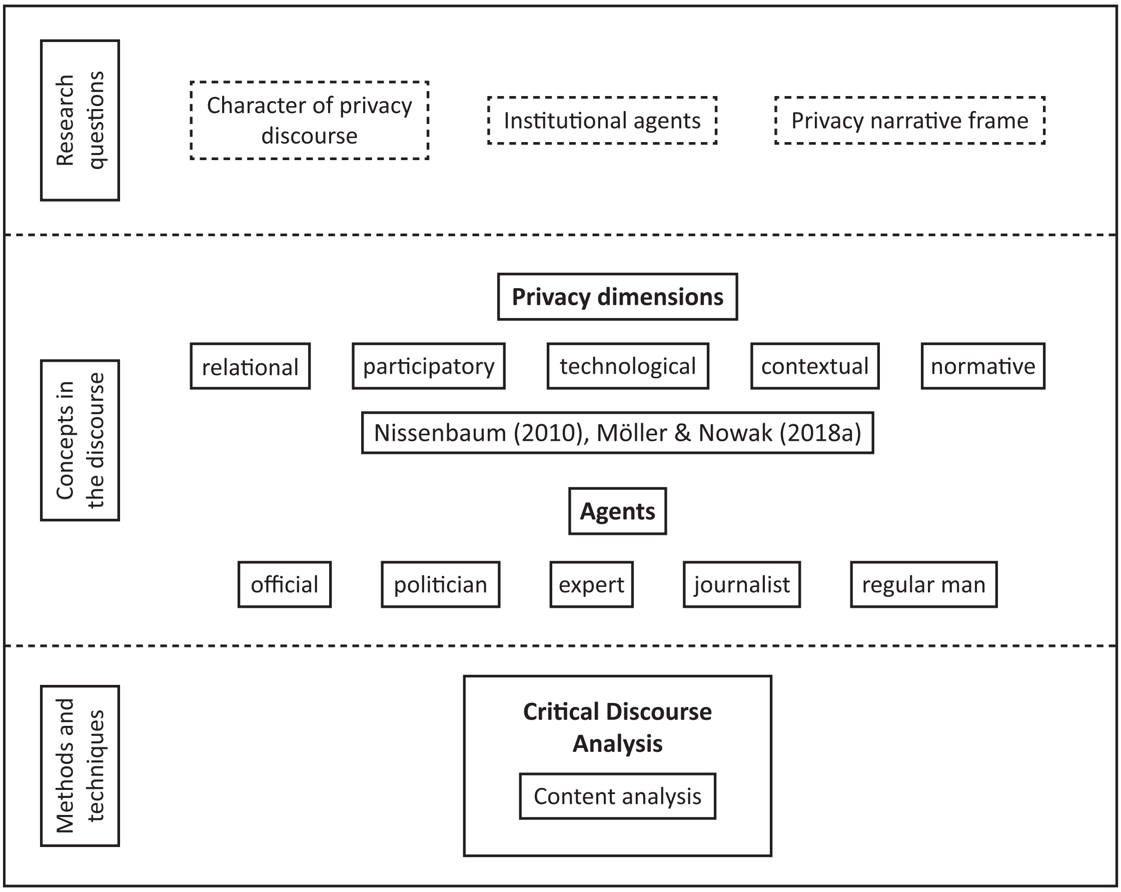


**Figure 1.** Analytical framework.

general privacy-related ongoing debates. This timetable was selected because of two case-related purposes. The first was the initiation of the GDPR debate in Poland. However, to capture its development, we started to collect the data from January 2018, a few months before the GDPR peaked. The second issue concerns the final case of FaceApp that saturated the discourse on privacy in September 2019.

Secondly, based on this we defined 12 issue-oriented categories. These are described in Table 1.

Thirdly, we conducted a quantitative and qualitative content analysis of media publications covering the 12 selected categories from January 2018 to September 2019. CDS approaches to text analysis and sampling are directed by the research questions (Bennett, 2018; cf. Unger et al., 2016). Thus, in order to capture the general character of the discourse on privacy, especially its dimensions, agents and frames, we used the purposive sampling. As the result, we collected a full sample composed of 169 texts from the websites of two newspapers (*Gazeta Wyborcza* [*GW*] and *Fakt*), two weekly political magazines (*Polityka* and *Wprost*), and two online news portals (wp.pl and wPolityce.pl). Media outlets were chosen according to the highest readership and popularity rates, and differences in editorial slant, both political and economic. Then, we used content analysis to extract the specific codes and linguistic categories of the texts (see Supplementary File) to reflect the five concepts of privacy: Relational, participatory, contextual, technological, and normative. Since the dynamic nature of discourse, these concepts are often collocated in particular texts. To complement the discursive construction of privacy dimensions with the institutional component, we distinguished five concepts related to institutional actors that shape the media discourse: Officials, politicians, experts, journalists, and the regular man. These concepts and their intersections are analysed in Section 4. What is important in terms of CDS framework, is that particular text excerpts are analysed to capture certain ways of argumentation and narrative frames (cf. Jäger, 2002; Wodak, 2002).

## 4. Research Results

### *4.1. The Character of Polish Privacy Discourse and Its Dimensions*

Both quantitative and qualitative analysis indicates four main issues in terms of the character of Polish media discourse on privacy. The first one concerns the manifestations of privacy dimensions. Due to the historical experience of Poland and the invasive politics of the government, as well as the interest in privacy protection declared by citizens, we expected that the Polish dis-

**Table 1.** Issue-oriented categories.

| Category | Description |
|---|---|
| GDPR | In Polish abbreviated as RODO |
| Uber Lex | A plan of changes in the Road Transport Act where the main issue concerned every driver who provides services related to the transport of persons must meet specific criteria, including usage of a mobile application that collects passengers data |
| Police Directive | A case related to the implementation of EU regulations, and related to the protection of personal data as part of actions taken to fight and prevent crime |
| Failure of government IT systems | I.e., epuap.gov.pl (an e-administration platform) |
| Central list of banned domains | A government initiative to create a register of banned domains (ultimately the project was not implemented due to non-compliance with EU law) |
| National Cyberarmy | The establishment of a Polish cyber military unit |
| Morele.net | The leakage of users' personal data |
| Government Center for Security | Fake text messages signed by Government Centre for Security announcing widespread mobilization |
| The Ministry of Digital Affairs and Facebook agreement | The Ministry of Digital Affairs and Facebook have signed an agreement on blocking accounts containing undesirable content |
| Facebook data leakage | Data breach of 50 million accounts on Facebook in September 2018 |
| The termination of Google's contract with Huawei | Due to the US legal concerns over Huawei equipment, Google terminates the Android support license on the Huawei smartphones |
| FaceApp | The introduction of the FaceApp mobile application |

course would have a participatory and relational, that is, citizen-oriented dimensions. Meanwhile, the most explicit in the Polish media discourse was the contextual (58.3%), technological (49.4%), and normative (48.8%) dimension of privacy. A relatively equal distribution of these dimensions in the sample resulted in a lower representation of the relational dimension (36.3%) and the participatory one (12.5%). The results indicate that the normative dimension was mainly based on EU privacy policy proceedings that form a top-down legal norm rather than a citizen/user-oriented data privacy 'manual.' Crucially, normative and participatory dimensions are only co-present in 10 (from 169) articles.

Secondly, data show that the Polish media discourse on privacy is strongly oriented to the legal and formal aspects of privacy. Thus, it addresses the application of EU-level privacy policy in Poland and general legal proceedings. The distribution of particular topics in the examined period indicates that the theme most often discussed in the context of privacy was GDPR (46.5%), followed by Facebook users' data leakage (7.6%), Lex Uber (7%), and the termination of Google's agreement with Huawei (7%) (see Figure 2). Importantly, the subject of GDPR was the most popular issue in the entire analysed period. Surely, the introduction of the GDPR invigorated the debate on privacy in Poland, yet it also strengthened the formal and legal nature of the discourse limiting the same time more user-oriented bottom-up approaches to privacy and data protection.

Thirdly, the media discourse on privacy was not polarized as one would expect concerting media divisions. The issue of privacy is mainly discussed in the dailies (*GW*—22.5%, the tabloid *Fakt*—21.3%) and online news portals (wpolityce.pl—23.7%, wp.pl—15.4%). Thus, as a consequence, the issues of complex privacy-related legal changes were communicated as news (65.7%). Meanwhile, columns that allow for a more descriptive and analytical form were much less used (21.3%). One would expect that the media discourse in which the participatory dimension of privacy is emphasized requires a more opinionated contribution. This finding is likely to have been an effect of publication frequency, with weeklies having the lowest ratio (*Polityka*—8.9%, *Wprost*—8.3%). Moreover, the relational, participatory and technological dimensions of privacy were observed more frequently in liberal outlets, like *GW*. It is worth to add that *GW*, *Polityka*, and wp.pl present liberal slant both in terms of politics and the economy. Therefore, we expected that through their texts they would call for the protection of the privacy of the individual. On the other hand, the normative and contextual dimensions were more frequent in conservative outlets. Tabloid *Fakt*, wPolityce.pl and, to a lesser extent, *Wprost* promote a conservative worldview and statism in the approach to

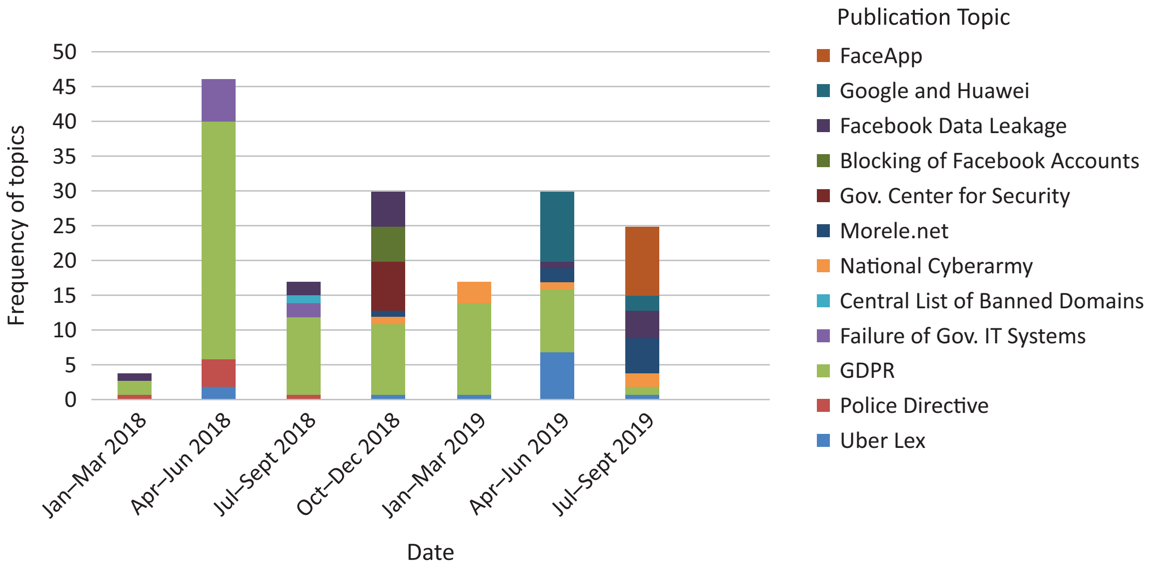


**Figure 2.** Frequency of privacy topics from January 2018 to September 2019.

the economy. Therefore, we expected the texts that indicate the important role of the state and its institutions in shaping the privacy policy. The results, however, indicate that the differences in addressing particular privacy dimensions are not significant in relation with political and economic slants of the medium. For instance, the participatory dimension was observed in 7.7% texts in liberal media to 4.8% in conservative (in terms of politics) and respectively 8.3% to 4.2% (in terms of economy). Normative dimension was observed in 21.4% of texts in liberal media to 27.4% in conservative (in terms of politics) and respectively 26.2% to 22.6% (in terms of economy). Thus, as in the case of political discourse in general, the privacy issues depend on editorial policies, although we are not able to conclude on media-related polarization.

Finally, privacy discourse was monopolised by news and informational function of the language used (observed in 89.3% of articles). However, a solid part of the texts was filled with expressive functions (in 37.5%) and persuasive (in 26.8%). Considering the saturation by metaphors (observed in 71.2% of the articles) and hyperboles (in 57.7%), the character of discourse on privacy may resemble the nature of political discourse in general in terms of its emotionality (cf. Balczyńska-Kosman, 2013).

### *4.2. Institutional Agents that Shape Privacy in Discourse*

Concerning the institutional agents that shape the Polish media discourse on privacy, it follows two main patterns. The first is institutional dispersal. Among the many agents that contribute to the discourse on privacy, government or public agencies and offices were presented by the Research and Academic Computer Network, CERT Poland, the Ministry of Digital Affairs, the Personal Data Protection Office, the Inspector General for the Protection of Personal Data, the Ministry of Infrastructure, and the Ministry of Internal Affairs and Administration. The expert side was presented inter alia by independent digital security experts, data security experts, Facebook, Niebezpiecznik (a data security and privacy advocacy collective and news website), Panoptykon (a countersurveillance and privacy advocacy NGO), lawyers and law firms (i.e., PwC consultancy firm), and Uber. Therefore, various institutions propose a different policy shaping the discourse on privacy in Poland. Journalists and experts contributed the most to the discourse in the period we examined (98.8% and 41.2%). Officials were framed less often, only in 26.1% of materials. The frequency of politicians' statements was only 9.7%. That observations are significant in the context of today state's privacy-invasive privacy politics. On the one hand, lack of commitment in the way of creating the discourse about privacy can be a deliberate action of state institutions that distract the public opinion from the crucial privacy issues. On the other hand, the low presence of politicians may indicate that the issue of privacy is not perceived as a part of a significant political struggle but rather as a specific policy that is the consequence of legal regulations.

Secondly, the intersection of institutional agents and privacy dimensions indicates that politicians, officials, and experts mostly addressed the contextual, technological and normative dimensions of privacy, leaving a participatory on the lowest level (see Table 2). Yet, the contextual dimension triggered by political actors does not refer to the specific political affairs but rather to the legislative context of applying EU law in Poland. The participatory dimension is most common among journalists (12.8%), slightly less among experts (7.3%). However, it mostly reflects legal arrangements and, besides a few excerpts, does not enhance the user participation in terms, for instance, data protection. Officials (3.7%) and politicians (0.6%) almost bypassed participatory issues, hence,

**Table 2.** Relation between institutions and dimensions of privacy (%).

| | | | Dimension | | | | | Total texts sum |
|---|---|---|---|---|---|---|---|---|
| | | | Relational | Participatory | Technological | Normative | Contextual | |
| Institution | Official | n | 15 | 6 | 18 | 19 | 27 | 43 |
| | | % total | 9.1% | 3.7% | 11.0% | 11.6% | 16.5% | 26.2% |
| | Politician | n | 3 | 1 | 10 | 10 | 10 | 16 |
| | | % total | 1.8% | 0.6% | 6.1% | 6.1% | 6.1% | 9.8% |
| | Expert | n | 31 | 12 | 37 | 36 | 39 | 68 |
| | | % total | 18.9% | 7.3% | 22.6% | 22.0% | 23.8% | 41.5% |
| | Journalist | n | 58 | 21 | 82 | 80 | 95 | 162 |
| | | % total | 35.4% | 12.8% | 50.0% | 48.8% | 57.9% | 98.8% |
| | Regular man | n | 2 | 2 | 3 | 3 | 8 | 10 |
| | | % total | 1.2% | 1.2% | 1.8% | 1.8% | 4.9% | 6.1% |
| Total | | N | 60 | 21 | 81 | 81 | 97 | 164 |
| | | % total | 36.6% | 12.8% | 49.4% | 49.4% | 59.1% | 100.0% |

it confirms the previous traces about distracting the public opinion or not considering privacy as political. At the same time, it indicates that the participatory dimension of privacy may not an element of the state's public communication in general. The normative dimension, likewise to the contextual, was framed mostly by journalists (48.8%), experts (22%), and officials (11.6%) leaving politicians with 6.1%. The institutional framing of a norm on privacy refers to a top-down perspective where the state's (for instance in GDPR case) and corporate policies (for instance Facebook or Google cases) communicate what citizens are committed to doing in regard to privacy. Norms are, thus, reduced to being legal rules without alternative for citizens who are rather believed to obey what is imposed upon them.

### *4.3. Discursive Narrative Frames of Privacy Policy*

This correlation between institutions and dimensions was analysed in terms of narrative frames that particular agents used shaping the discourse. The analysis indicates three main discursive narratives concerning framing privacy policy by institutional actors. Firstly, as previously demonstrated, the media discourse was mostly framed with the formal narrative based on legal procedures bypassing political aspects of privacy. For instance, texts that focus mostly on the normative dimension are dominated by frames of "regulations," "proceedings," "legal frameworks," and "data processing," often using formal language and informational style captured in formal legal-based discursive manner:

> Later in the autumn of 2017, the assumptions to the amendment to the Act on the provision of electronic services have been prepared, pursuant to which Facebook could no longer make arbitrary decisions on blocking accounts. (Czubkowska, 2018)

> Personal Data Protection Office…has to check whether GDPR regulations will be respected. Penalties can be severe because companies are threatened with fines of up to 20 million euros. (Kowanda, 2018)

> Today, the police and the prosecutor's office process our data on the principles set out in the Personal Data Protection Act of 1997, and their operation is subject to the control of the Inspector General for the Protection of Personal Data. (Ivanova, 2018)

Other legal topics—for instance, Uber Lex, the establishment of a Polish National Cyberarmy, and the government agreement with Facebook—were mostly news pieces with short excerpts of official statements of the ministries framed in an informative manner to express involvement of particular institutions, for example: "As there is no legal path of appeal against the decision of social network platforms registered outside Poland, we decided to approach the problem from the administrative angle" (Bednarek, 2018).

Since analysis indicate that privacy-related issues are framed not as a field of political struggle and debate but rather as a policy to be implemented as a consequence of legal regulations, there were limited excepts where the politicians contributed to the discourse, for instance, in case of the GDPR:

> We collected over three thousand signatures, although a thousand fewer was enough. But two weeks of collecting signatures on the streets and in the markets made me realize that in the era of the GDPR, people do not want to provide their data to a person whom they do not know, and to sign the petition supporting the political committee, you need to provide your name, surname, address and PESEL. (Kursa, 2019)

Here and in the other articles on the GDPR, politicians perceive the new regulations as an obstacle to electoral campaigning that they try to find an administrative solution for. For example, GDPR is closed in a frame of an epochal regulation: 'the era of GDPR.' The politician shares his concern of the issue of private data that could be shared 'to a person whom they don't know,' hence he poses himself as the 'stranger,' a person of limited trust. In the initial phrase, the politician claims that despite GDPR they 'collected over three thousands signatures, although…' using at same time the narrative of active involvement that refers to frame *us versus them*, politicians versus common people who are not willing to support the committee or provide the private data.

A second narrative frame refers to polarisation and contrasting concerning relations of users and the state or corporations. In the following excerpts, the contradiction between users' rights and capabilities in relation with Facebook serves as a crucial narrative juxtaposition:

> It's really not difficult to violate community rules or Facebook regulations. This happens every day to political activists, organizers of assemblies, social organizations and ordinary users. (Szymielewicz, 2018)

> The way to restore a blocked account or content more resembles a fruit machine than an objective tribunal. All protests of blocked users go into one bag. Just one click is enough. Facebook gives everyone who is unsatisfied a simple interface but denies them the right to speak. The user has no place to write why he thinks that his content or account has been unjustly blocked. An activist to whom the portal took the work tool, presses the same button as the "regular user" who was cut out from part of a social conversation. They both wait for the machine to grind through the protest and spit out something. The effect of the grinding is either to remove the block (without a word of explanation) or the decision to maintain it (also without a word of explanation). (Szymielewicz, 2018)

On the one hand, a tech company is framed with metaphors of 'fruit machine,' 'waiting for the machine to grind' or the 'private censorship' that is used in the title of the article to describe the social media platform's arcane decision-making process. On the other hand, a frame used to capture users' weaker position in relation to tech companies is deployed: 'protests of blocked users go to one bag' metaphor, 'regular users' neologism or 'violation of community rules or Facebook is really not difficult. Every day it happens to political activists, assembly organizers, social organizations and ordinary users' later in the same article. Thus, in this case, normative and participatory dimensions intersected with the institutional actors justify the bottom-up perspective in privacy-oriented norm by ascribing negative attributions through metaphors to tech companies.

However, 7 of the 10 articles that intersect normative and participatory dimensions address issues of the GDPR using a narrative of trivialising by referring to the absurdity of its implementation: "Hospitals and clinics have been made stupid by the GDPR" (Watoła, 2018), "GDPR at school. Student number five, acknowledge receipt of the test" (Warchała, 2018), or "Besides, most of what the media call the *absurdities* of the GDPR results from incomplete knowledge of the rules by administrators and an excessive zeal often caused by fear of high penalties" ("Absurdy RODO," 2018). In general, the sample frequently zooms in onto the frame of "banality" of the GDPR. The norm is again framed around the notion of legal relation between particular institutions and citizens that need to follow the rule that is "banal." Thus, the narrative of trivialising labelled with the frame of "banal" regulation, undermines the participatory and relational dimensions by reinforcing top-down privacy order and inequality between tech company and users.

Thirdly, there were only a few cases where the narrative frame enhanced the privacy of citizens/users and put forward a bottom-up privacy policy. In such cases, the narrative frame of intensification was deployed in addressing the normative dimension and to some extent participatory one. For instance, a solely participatory dimension of privacy was referred to in the articles on data leakages, i.e., from Facebook and the online shop Morele.net:

> What should you do if you are on the list (of leaked Morele.net data—Authors)? If your email address was on the displayed list, change your password immediately. It is also a good idea to use the already popular two-step authorization option. In most cases this should help. If your email has a good spam filter, there is a chance that you will never realize that your address has been stolen. ("Ze sklepu morele.net," 2019)

Such a 'privacy tutorial' based on a *do it yourself* intensification narrative frame was characteristic for pieces on building data-privacy awareness in the discourse in a bottom-up manner. Privacy policies were directly addressed to the users ("you," "your") and aimed at either protection of their data or to raise awareness of technological issues concerning privacy, as in the Google/Huawei case. It was framed with direct indications to intensify privacy practices: "change your password immediately," "good idea to use," "should help." The evidence, however, indicates that only a few excerpts in the entire sample offer a user-oriented approach to privacy policies.

Similarly, the case of FaceApp follows such a narrative frame. The worldwide popularity of FaceApp also effected the Polish discourse on privacy. Importantly, it addressed the privacy issue not just as a legal, EU-related process, but as a user-oriented "tutorial" of data protection that forms privacy policy of sorts. In the sample, this issue was constructed as predominantly being tackled by officials, experts and journalists. Discursively, the FaceApp case was framed in multiple narrative schemes. From informative lines describing basic functions of the app, through to the frame of "danger" and "threat," as in tabloid daily *Fakt*: "FaceApp, the record-breaking Russian mobile app for Apple iOS devices threatens users' privacy, inter alia by sending their photos directly to the cloud servers of the app creators who make them available to the external entities" ("Popularna aplikacja,'' 2019).

There were also some contextual opinions, referring to previous privacy threats and data-security analysis and detailed case studies of users' privacy online practices:

> The Poles checked whether the application is secure….CERT Poland experts examined the conduct of the FaceApp application, which aroused both huge interest and considerable controversy last week. Experts have analysed this software to see if it actually allows for "stealing" data. (Breczko, 2019)

Finally, it was critically framed in the discourse from a normative perspective by Katarzyna Szymielewicz (Panoptykon president):

> We feed data algorithms without reflection, without knowing and being able to predict for what purpose their ability to recognize our biometric features and behaviour modelling—from how we move, what and when we buy—will be used by commercial companies and states that use their knowledge. If you react with slight anxiety to the line "Russian application," I encourage you to remain sceptical about any applications that give you something trivial in exchange for valuable data. (Szymielewicz, 2019)

Importantly, with limited knowledge about the actual operations of FaceApp, the initial narrative frame used by state officials was convergent with the "danger" and "threat" scheme connected directly to Russian disinformation strategies, thus "Russian" and its collocation serves in the discourse as a negative label used to deprecation but also as a form of argumentation strategy aimed in justification of negative attribution ascribed to Russia (cf. Lokot, 2020). Yet, over time the narrative frame of perspectivation was deployed with references to experts and their research on the actual function of the application. It shifted the discourse into the more data-based perspective in building a specific norm of privacy captured in frames of, for instance: "CERT Poland experts," "experts have analysed" (Breczko, 2019). Finally, the expert's analysis triggered the normative dimension to frame the norm. On the one hand, the excerpt starts with the frame that justify the imbalance between the users who "feed data algorithms without reflection" and the tech companies referring to users' incompetence and emotions: "without reflection" or "without knowing" and "slight anxiety" (Szymielewicz, 2019). On the other hand, the narrative frame deploys the intensification of a norm coined in user-oriented call to "encouragement" or being "sceptical." As analysis indicates, the normative frame referred to a crucial data privacy and surveillance issues. However, this frame was triggered the most not by the user-oriented concerns but rather as the issue imposed from a top-down perspective as in the FaceApp case.

## 5. Discussion and Conclusion

Privacy is articulated both in terms of policy and politics. Concerning the general character of Polish media discourse, contemporary politics and the historical settings, we would have expected polarized debate with strong references to the communist past. Instead, it seems that Polish debates on privacy are driven by contemporary European politics. Indeed, some data prove the rise of the awareness and good practices in the field of privacy protection in last decade, but the same time 59% of respondents in Poland have not heard of privacy-invasive practices, i.e., data collection, of state or government entities (European Commission, 2015). Despite the fact that Poles declare that the protection of privacy is a very important issue, the research conducted after the implementation of the GDPR shows that 40% of respondents have not heard about the GDPR at all ("Polacy, bez szerszej wiedzy o RODO," 2018). Therefore, when taking up the problem of the specifics of the discourse on privacy in Poland, we were interested in assessing its nature, i.e., whether it is focused on increasing citizens' awareness and knowledge and giving a kind of know-how when it comes to privacy practices.

Three crucial issues characterise the Polish media discourse on privacy. Firstly, participatory and relational aspects of privacy are hardly present. It may seem surprising given the communist mass surveillance past and surveillance current state's politics. Thus, concerning privacy dimensions, the relation between citizen and the state is norm-based, the norm is almost entirely legal, and the citizens' participation is purely data-oriented and limited. In terms of the topic referential frame, the results of our research have shown that the discourse on privacy is dominated by the legal aspects. Moreover, the topic of privacy was primarily related to the EU privacy policy and the GDPR is the most common topic in the narrative throughout the entire analysed period. The emerging privacy discussion in Poland was triggered by external factors and not by internal debates on the importance of privacy in political contexts. As a consequence, the media discourse was primarily informative, focused on mainly framing legal aspects of privacy policies, which is related to the specificity of the procedural issue concerning, e.g., GDPR, Lex Uber, the Cyberarmy, and Facebook regulations.

Secondly, our research shows the variety of institutional agents that shape privacy media discourse.

Apart from journalists, who naturally participate in media debates, the experts and their institutions framed the privacy policy debate (including independent digital security and data security experts, Facebook officials, Niebezpiecznik workers, Panoptykon, PwC, Uber, Bolt, etc.). Representatives of the state institutions and politicians were much less frequently present in the sample, despite the fact that the discourse was tilted towards the legal framework of privacy policies. It may indicate that privacy is not perceived as political or state's representatives may also not be interested in firming privacy-conscious public opinion. Thus, the thematic frame confirms that multiple official institutions dealing with privacy regulations, often do not mention 'privacy' at all. The study shows limited evidence that privacy policies present in the media discourse form a norm regarding how to deal with privacy and data protection when it comes to the actual online environment. Moreover, this is led by experts rather than official institutions. If any privacy norm is pursued, it is rather not citizen-oriented but captures the legal relations of state and public/private institutions or public/private institutions with the citizen. Instead of discussions on how to enhance privacy within such a dynamic information environment, as is the case in Germany (cf. von Pape et al., 2017), the Polish media discourse mainly reflected the formal aspect bypassing the context of state's privacy-invasive privacy politics.

Thirdly, the intersection of privacy dimensions and institutional agents that form discourse on privacy was particularly important to our study. Thus, we have analysed particular excerpts to see what narrative frames and with what linguistic tools were deployed. The critical discourse analysis confirms the domination of formal narrative frame focused on legal-based proceedings. Its formality is shaped with an informational report that reinforces the top-down approach to privacy or is accompanied by trivializing narrative using 'banal' frame to capture the legal regulations. Moreover, the juxtaposition narrative slants the frame of inequality between positively labelled users and tech companies labelled negatively. It follows an argumentation strategy used to justify the labels of users' exclusion and their unequal position in the discourse. It, to some extent, resembles the polarisation tendencies of Polish political discourse in general (cf. Balczyńska-Kosman, 2013). However, in building the normative take to privacy, institutional actors (experts) deploy the intensification frame in a more user-oriented manner to mitigate a more bottom-up privacy policy. Yet, these attempts were limited. Instead of targeting the issues of privacy as essential to Polish historical and current political drive, experts and politicians refer to privacy as something "imposed on us" from the outside, whether this is EU regulation or tech company affairs.

Concerning the historical development of privacy in a post-communist country, the media discourse indicates that privacy still resembles the omnipotent control of the state (or the corporation) that tells citizens "what to do" in terms of the entering the legal proceedings. Yet without improving citizens' privacy when it comes to relation with the state or corporation. Concerning the contemporary privacy-invasive politics of the state, the analysis illustrates that privacy is perceived as externally implemented and do not relate to political issues. Thus, privacy policy framed in the discourse does not normalise the relation between the state and the citizen. Apart from the Facebook and government agreement this rarely refers to any specific norm on privacy policy in the participatory dimension. As a result, the privacy policy in Polish discourse reframes or repackages a patchwork of often unrelated narratives reflecting multiple institutions that try to "translate" legal norms to citizens instead of enhancing them with actual awareness and data-privacy skills.

## Acknowledgments

The authors would like to express the gratitude the Department of Communication, Media and Journalism at Nicolaus Copernicus University in Toruń for the financial support and the student assistants for their research input on the initial stages of the project.

## Conflict of Interests

The authors declare no conflict of interests.

## Supplementary Material

Supplementary material for this article is available online in the format provided by the authors (unedited).

## References

Absurdy RODO wynikają z nieznajomości prawa [GDPR absurdities arise from ignorance of the law]. (2018, November 25). *wPolityce*. Retrieved from https://wgospodarce.pl/informacje/56819-absurdy-rodo-wynikaja-z-nieznajomosci-prawa

Balczyńska-Kosman, A. (2013). Język dyskursu publicznego w polskim systemie politycznym [Language of public discourse in the Polish political system]. *Środkowoeuropejskie Studia Polityczne*, *2013*(2), 143–153.

Bednarek, A. (2018, November 28). Zbanowali cię na Facebooku? Ministerstwo Cyfryzacji pomoże. Jako pierwsze na świecie [They banned you on Facebook? The Ministry of Digital Affairs will help. As the first in the world]. *WP*. Retrieved from https://tech.wp.pl/zbanowali-cie-na-facebooku-ministerstwo-cyfryzacji-pomoze-jako-pierwsze-na-swiecie-6321823758816897a

Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: MIT Press.

Bennett, S. (2018). *Constructions of migrant integration in British public discourse: Becoming British*. London: Bloomsbury Academics.

Breczko, B. (2019, July 23). FaceApp. Polacy sprawdzili, czy aplikacja jest bezpieczna [FaceApp. The Poles checked whether the application is secure]. *WP*. Retrieved from https://tech.wp.pl/faceapp-polacy-sprawdzili-czy-aplikacja-jest-bezpieczna-6405620686218881a

Centrum Badania Opinii Społecznej. (2016). *Inwigilacja w internecie* [Surveillance on the Internet] (Report No. 72/2016). Warszawa: Fundacja Centrum Badania Opinii Społecznej.

Centrum Badania Opinii Społecznej. (2018). *Bezpieczeństwo w internecie* [Security on the Internet] (Report No. 133/2018). Warszawa: Fundacja Centrum Badania Opinii Społecznej.

Czubkowska, S. (2018, November 28). Zablokował cię Facebook? Ministerstwo Cyfryzacji pomoże. Serwis Zucerberga ugina się pod naciskiem rządów [Facebook blocked you? The Ministry of Digital Affairs will help. Zuckerberg's website is bending under government pressure]. *Gazeta Wyborcza*. Retrieved from https://wyborcza.pl/7,156282,24218971,facebook-ugina-sie-pod-rzadami-takze-polskim.html

Czyżewski, M., Kowalski, S., & Piotrowski, A. (2010). *Rytualny chaos: Studium dyskursu publicznego* [Ritual chaos: A study of public discourse]. Warszawa: WAiP.

European Commission. (2015). *Special Eurobarometer 431: Data protection*. Brussels: European Commission. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

Gorwa, R. (2017). *Computational propaganda in Poland: False amplifiers and the digital public sphere* (Working Paper No.2017.4). Oxford: Oxford University. Retrieved from https://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Poland.pdf

Ivanova, E. (2018, February 27). Dyrektywa policyjna musi być wdrożona do 6 maja. Jeśli Polska nie zdąży, nie będzie kontroli nad zbieraniem danych obywateli [The police directive must be implemented by May 6. If Poland fails on time, there will be no control over the collection of citizens' data]. *Gazeta Wyborcza*. Retrieved from https://wyborcza.pl/7,75398,23074697,dyrektywa-policyjna-musi-byc-wdrozona-do-6-maja-jesli-polska.html

Jäger, S. (2002). Discourse and knowledge: Theoretical and methodological aspects of a critical discourse and dispositive analysis. In R. Wodak & M. Meyer (Eds.), *Methods of critical discourse analysis* (pp. 32–62). London: SAGE.

Kowanda, C. (2018, June 5). RODO na łapu-capu [GDPR in a hurry-scurry]. *Polityka*. Retrieved from https://www.polityka.pl/tygodnikpolityka/rynek/1750974,1,rodo-na-lapu-capu.read

Kubitschko, S. (2018). Acting on media technologies and infrastructures: Expanding the media as practice approach. *Media, Culture & Society*, *40*(4), 629–635. http://doi.org/10.1177/0163443717706068

Kursa, M. (2019, September 2). Wybory parlamentarne 2019: W dobie RODO coraz trudniej o podpisy z poparciem [2019 Parliamentary elections: In the age of the GDPR, it is becoming increasingly difficult to collect the signatures of support]. *Gazeta Wyborcza*. Retrieved from https://krakow.wyborcza.pl/krakow/7,44425,25149014,wybory-parlamentarne-2019-w-dobie-rodo-coraz-trudniej-o-podpisy.html

Lokot, T. (2020). Data subjects vs. people's data: Competing discourses of privacy and power in modern Russia. *Media and Communication*, *8*(2), 314–322.

Meissner, F., & von Nordheim, G. (2018). Exploration of a fragmented discourse. Privacy and data security in Süddeutsche Zeitung: 2007–2017. *Mediatization Studies*, *2018*(2), 103–123. https://doi.org/10.17951/ms.2018.2.103-123

Möller, J., & Nowak, J. (2018a). Surveillance and privacy as emerging issues in communication and media studies. An introduction. *Mediatization Studies*, *2018*(2), 7–15. http://dx.doi.org/10.17951/ms.2018.2.7-15

Möller, J., & Nowak, J. (2018b). Don't hate the media: Act on media. Civil society agents' media-oriented practices on encryption/privacy. [PowerPoint presentation].

Möller, J., & von Rimscha, M. B. (2017). (De)centralization of the global informational ecosystem. *Media and Communication*, *5*(3), 37–48. http://dx.doi.org/10.17645/mac.v5i3.1067

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

Polacy, bez szerszej wiedzy o RODO—sondaż ARC Rynek i Opinia [Poles, without broader knowledge about the GDPR—ARC market and opinion poll]. (2018, May 8). *Rzeczpospolita*. Retrieved from https://www.rp.pl/Dane-osobowe/305089958-Polacy-bez-szerszej-wiedzy-o-RODO---sondaz-ARC-Rynek-i-Opinia.html

Popularna aplikacja może być niebezpieczna [A popular application can be dangerous]. (2019, July 18). *Fakt*. Retrieved from https://www.fakt.pl/wydarzenia/polska/popularna-aplikacja-faceapp-zagraza-prywatnosci-uzytkownikow/6tb17ln

Ptaszek, G. (2018). Surveillance capitalism and privacy: Knowledge and attitudes on surveillance capitalism and online institutional privacy protection practices among adolescents in Poland. *Mediatization Studies*, *2018*(2), 49–68. http://dx.doi.org/10.17951/ms.2018.2.49-68

Sojka, A. (2013). *Poland: A surveillance Eldorado? Security, privacy, and new technologies in Polish leading newspapers (2010–2013)* (Seconomics Discussion Papers 2013/3). Prague: Institute of Sociology, Czech Academy of Sciences. Retrieved from https://www.soc.cas.cz/sites/default/files/soubory/poland_-_a_surveillance_eldorado.pdf

Svenonius, O., & Björklund, F. (2018). Explaining attitudes to secret surveillance in post-communist societies. *East European Politics*, *34*(2), 123–151. https://doi.org/10.1080/21599165.2018.1454314

Szumańska, M., Klicki, W., Niklas, W., Szymielewicz, K., & Walkowiak, A. (2016). *Zabawki wielkiego brata, czyli krótki przewodnik po narzędziach, które pomagają państwu kontrolować obywateli* [Big brother toys, or a short guide to the tools that help the state control the citizens]. Warszawa: Fundacja Panoptykon.

Szymielewicz, K. (2018, November 30). Co rząd wynegocjował z Facebookiem? „Noga w drzwi" prywatnej cenzury [What the government negotiated with Facebook? 'Leg in the door' of private censorship]. *Polityka*. Retrieved from https://www.polityka.pl/tygodnikpolityka/kraj/1773606,1,co-rzad-wynegocjowal-z-facebookiem-noga-w-drzwi-prywatnej-cenzury.read

Szymielewicz, K. (2019, July 18). „Rosyjski" FaceApp nie jest groźniejszy od samego Facebooka ['Russian' FaceApp is not more dangerous than Facebook itself]. *Polityka*. Retrieved from https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1800964,1,rosyjski-faceapp-nie-jest-grozniejszy-od-samego-facebooka.read

Unger, J., Wodak, R., & KhosraviNik, M. (2016). Critical discourse studies and social media. In D. Silverman (Ed.), *Qualitative research* (pp. 1170–1241). London: SAGE.

von Pape, T., Trepte, S., & Mothes, C. (2017). Privacy by disaster? Press coverage of privacy and digital technology. *European Journal of Communication*, *32*(3), 189–207. https://doi.org/10.1177%2F0267323117689994

Warchała, M. (2018, June 13). RODO w szkole. Uczniu numer pięć, pokwituj odbiór klasówki [GDPR at school. Student number five, acknowledge receipt of the test]. *Gazeta Wyborcza*. Retrieved from https://katowice.wyborcza.pl/katowice/7,35063,23530236,uczniu-numer-piec-pokwituj-odbior.html

Watoła, J. (2018, July 28). Szpitale i poradnie ogłupiały przez RODO. Także na Śląsku [Hospitals and clinics have been stupid by the GDPR. Also in Silesia]. *Gazeta Wyborcza*. Retrieved from https://katowice.wyborcza.pl/katowice/7,35063,23726738,szpitale-i-poradnie-oglupialy-przez-rodo-takze-na-slasku.html

Westin, A. F. (2015). *Privacy and freedom*. New York, NY: IG Publishing.

Wodak, R. (2002). The discourse historical approach. In R. Wodak & M. Meyer (Eds.), *Methods of critical discourse analysis* (pp. 63–94). London: SAGE.

Ze sklepu morele.net wyciekły dane 2,5 mln użytkowników. Sprawdź, czy jesteś na liście [Data from 2.5 million users leaked from the morele.net store. Check if you are on the list]. (2019, April 22). *Wprost*. Retrieved from https://biznes.wprost.pl/firmy-i-rynki/10210459/ze-sklepu-morelenet-wyciekly-dane-25-mln-uzytkownikow-sprawdz-czy-jestes-na-liscie.html

## About the Authors

**Łukasz Wojtkowski** (PhD) is Assistant Professor in the Department of Communication, Media and Journalism at Nicolaus Copernicus University in Toruń. He's the Author of books on mediatization of politics and culture, peer-reviewed articles and book chapters on mediatization, digital cultures, and technology. His research interests focus on critical theory and mediatization; privacy, surveillance, and disinformation; and critical discourses.

**Barbara Brodzińska-Mirowska** (PhD) is Assistant Professor in the Department of Communication, Media and Journalism at Nicolaus Copernicus University in Toruń. Her science interests are focused on political communication, public relations, political reputation, the role of new communication technologies in political communication, and mediatization of politics. She is the Author and Co-Author of books and articles related to party politics communication activities, professionalization of political communication and new media.

**Aleksandra Seklecka** (PhD) works as Associate Professor in the Department of Communication, Media and Journalism at Nicolaus Copernicus University. She is a Political Scientist and a Sociologist. She is the Author of over 30 articles and several books about media manipulation, political marketing, and reports on the relations between politics and mass media. Her interests focus on Polish media system and ritual communication.

COGITATIO

**Media and Communication (ISSN: 2183–2439)**
**2020, Volume 8, Issue 2, Pages 314–322**
**DOI: 10.17645/mac.v8i2.2883**

Article

# Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia

Tetyana Lokot

School of Communications, Dublin City University, Dublin 9, Ireland; E-Mail: tanya.lokot@dcu.ie

Submitted: 9 February 2020 | Accepted: 5 May 2020 | Published: 23 June 2020

**Abstract**
The notion of individual privacy has always been a political one throughout Russia's Soviet and post-Soviet periods, but in the age of all-encompassing datafication and digitisation of identities, privacy has become an even more contested concept. This article considers how Russian state officials and Russian digital rights advocates construct the notion of privacy in their public online discourses. I argue that how these actors talk about privacy helps shape the norms and the politics around it in Russia. An in-depth analysis of activity reports published online by the state internet regulator and a grassroots digital rights group reveals competing privacy discourses underpinned by differential understandings of how anonymity, secrecy, confidentiality, and control of personal data determine the distribution of power and agency in Russian public and political life. These differential interpretations of privacy inform the contentious politics that emerge around how privacy is regulated and negotiated within the greater regulatory and normative framework of digital citizenship in Russia. Thus, the article offers critical insights into the contestation of citizenship and, consequently, the distribution of power in more and less democratic systems.

**Keywords**
data; digital rights; power; privacy; Russia

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

## 1. Introduction

With digital technologies and networked internet platforms firmly embedded in the mainstream political and social life, and amid increasing datafication (Mayer-Schönberger & Cukier, 2013; Van Dijck, 2014) of all facets of society and identity, media and communications scholarship is increasingly concerned with how these forces are shaping the distribution of power and agency among the various actors involved in this ecosystem. This study focuses on the notion of privacy in the networked era and the emerging politics around it as closely related to issues of control, power, and agency. Examining the case of Russia, I argue that certain state and non-state actors engage in public discourse to articulate competing conceptions of privacy politics, and that these discursive articulations underpin different visions of how agency, power, and control should be distributed in a datafied society. Capturing these divergent ideas can offer valuable insights about how the state and citizens in Russia—and other networked authoritarian states—understand the meaning of privacy and its place in the emergent construction of digital citizenship.

Section 2 charts the development of the concept of privacy in media and communications scholarship, underscoring the highly contextual, relational, and political nature of privacy in technological systems and mediated environments. This section then discusses the understanding of privacy in the Russian context, and how the concept has evolved from the Soviet era to the modern times. The study then presents arguments for examining the discursive representations of privacy as a way of understanding the competing politics of privacy in Russia today.

Section 3 briefly introduces the two sources of privacy discourse in this study: the Russian state regulator Roskomnadzor (RKN) and the digital rights group Roskomsvoboda (RKS). It then outlines the collection of publicly available activity and monitoring reports produced by both organisations and describes the approach used to analyse the privacy-related discourses that emerge from these public communications.

Section 4 presents an analysis of how both the state regulator and the digital rights group discursively construct privacy as contextual, relational, and political. The analysis suggests that the discursive representations of privacy by the state regulator and the digital rights activists are in competition with one another, and illustrates how this divergence informs the contentious politics of privacy in Russia.

Lastly, Section 5 presents concluding thoughts about the competing discursive articulations of privacy and the resulting politics of privacy in Russia, as reflected in the state's struggle for control over accessibility of private data and the grassroots resistance against restrictions of personal data flows. The section concludes with suggestions for future research by media and communication scholars into privacy politics and its discursive construction.

## 2. Articulating Privacy and Its Politics

This section first unpacks how the concept of privacy is discussed in media and communications scholarship. Next, it traces the evolution of the notion of privacy in Russian political and public life. Finally, it argues for the importance of attending to the discursive construction and representation of privacy by state and non-state actors as a vital force that shapes the politics of privacy in the Russian national context.

### *2.1. The Concept of Privacy in Media and Communications Scholarship*

Pinning down the exact definition or nature of privacy as a concept is an ongoing struggle within media and communications scholarship (and, for that matter, in other disciplines as well). Nissenbaum (2010, p. 2) suggests it is less useful to grasp whether privacy is "a claim, a right, an interest, a value, a preference, or merely a state of existence" than to trace the concerns related to privacy with regard to technological systems and digitally-mediated practices related to flows of personal information. Rather than arguing for privacy to be understood as a purely descriptive, normative, or legal concept, it seems more productive to examine how certain descriptions of privacy, norms, or regulations around it engender anxiety, resistance, or struggle for control over accessibility and/or restrictions of personal data flows.

Following Nissenbaum's (2010) logic, Möller and Nowak (2018) suggest that privacy can be best understood as contextual, relational, and political. They argue that in line with Nissenbaum's (2010) idea of "contextual integrity," privacy is best conceptualised and reconceptualised with regard to specific contexts. Further, privacy is not only understood in relation to individuals, but is realised or threatened as a constant process of strategic determination (Trepte et al., 2017; Westin, 2015) with regard to how their personal information flows between them and other individuals and institutions in society (Möller & Nowak, 2018). In this regard, privacy can also be understood as relational because it relates to and is informed by a multitude of other issues, from surveillance and control to anonymity, confidentiality, and security. Finally, privacy can be understood as political or participatory (Möller & Nowak, 2018), as increasingly privacy-related decisions and activity impact other actors in any individual's networks, and have implications for political participation, individual safety of dissidents (when coupled with surveillance), and the overall climate of political freedom and expression—or lack thereof—in both democratic and non-democratic societies. I posit, therefore, that the contextual and relational articulations of the politics of privacy are intrinsically connected to broader issues of power, agency, and control in the framework of digital citizenship as it is understood and performed by various actors, including states, platforms, media, and citizens.

### *2.2. Privacy in Russia's Networked Authoritarian State*

The notion of individual privacy has always been a political one throughout Russia's Soviet and post-Soviet periods, connected as it was to the culture of pervasive state surveillance (Lokot, 2018) and the struggle to control thoughts, opinions, and information flows in both public and private lives of citizens (Gorny, 2007). Reflecting on the Bolsheviks' view that anything private was deprived of social meaning and thus politically dangerous, Boym (1994, p. 73) concludes that in early Soviet Russia "personal life seems rather to fit a concept of publicly sanctioned guilt and of a heightened sense of duty." However, in the age of all-encompassing datafication and digitisation of identities, privacy has become an even more contested concept in Russia, given the citizens' embrace of digital technologies and the state's preoccupation with control over data and information flows as part of the national security and sovereignty project. This has led to the emergence of what Greene (2012, after MacKinnon, 2011) terms 'networked authoritarianism': a regime in which the state prioritises developing networked infrastructure and digital connectivity, while seeking to control all spheres of the datafied social life.

The term 'privacy' itself (*приватность* [privatnost] in Russian) is a term clearly borrowed from other languages (Levontina, Shmelev, & Zaliznyak, 2017) and a fairly recent addition to everyday Russian vocabulary, though other partial representations of it such as confidentiality, secrecy, and 'private life,' predate it (Boym, 1994). But privacy in the modern sense, including the privacy of personally identifying information, individual communications, behaviour, and digital data traces, is only now entering the mainstream legal, political, and social discourse in Russia. In legislative terms, for instance, this has meant that the traditional repertoire of legal protections for confidentiality of private communications and 'private life' has been expanded to include personal data protection (e.g., Federal Law "On Personal Data" [Russian Federation, 2006])—but also that access to user data and metadata stored by online entities and social media platforms is viewed by the state and law enforcement as a matter of national security (Soldatov & Borogan, 2013), while citizens increasingly perceive state policies in the area of data localisation (Sargsyan, 2016) and internet sovereignty (Lipman & Lokot, 2019) as threats to individual privacy. It is therefore important to investigate the competing representations of this concept in the Russian discursive public sphere and to capture how these competing forces in the field of privacy might reflect the overarching power struggles in society and represent competing ideas of the political power of the state and its citizens, spanning from hegemony to democracy.

### *2.3. Discursive Constructions of Privacy*

This article considers how the Russian state and Russian digital rights advocates construct competing notions of privacy in their public-oriented discourses. Subscribing to a post-structuralist, critical approach that sees discourses as never separate from reality, but possessing the power to co-create it (Fairclough, 2013), I argue that how these actors conceptualise and contextualise privacy in their communications with the public helps shape the politics around privacy in Russia. An in-depth analysis of the text corpora of regularly published activity and monitoring reports by the state internet regulator and one of Russia's most prominent grassroots digital rights groups points to competing privacy discourses, concerned with questions of how privacy is understood, what value it possesses, and how it is conveyed, controlled, or restricted. The discursively constructed politics of privacy, I argue, are underpinned by differential understandings of how anonymity, secrecy, confidentiality, and control of personal data determine the distribution of power and agency in Russian public life.

In addition to being an empirical study of the Russian context that contributes to Russia-focused literature on internet governance and free expression online, this article applies the analytical privacy framework developed by Möller and Nowak (2018) to discursive constructions of privacy. It thus aims to make a novel theoretical contribution to the media and communications scholarship on privacy by articulating the connections between how the politics of privacy is represented discursively and how its divergent representations shape internet regulation, freedom of expression online, and digital citizenship in Russia.

## 3. Research Design and Methods

Though specific legislative, political, and other practices on the part of the state and the digital rights activists may point to the competing notions of privacy in Russia, it is equally important to examine how state and civic actors articulate these ideas in discursive terms in digitally-mediated spaces. Therefore, I chose to examine publicly available activity reports produced by Russia's state internet regulator, RKN, and by RKS, one of Russia's most prominent digital rights groups, to understand how these communications are used to shape discursive representations of privacy.

RKN (also known as the Federal Service for Supervision of Communications, Information Technology and Mass Media) is the Russian federal executive body tasked with oversight, monitoring and censorship of electronic media, mass communications, information technology, and telecommunications (Turovsky, 2015). It operates as an independent agency under the auspices of the Ministry of Digital Development, Communications, and Mass Media. RKN oversees compliance with relevant Russian legislation and manages Russia's extensive banned websites registry.

The grassroots digital rights initiative whose privacy-related discourses I examine is RKS, one of the main digital rights advocacy groups in Russia. It was founded in 2012 by members of the Pirate Party in Russia (Merzlikin, 2019) to address the early crackdown on internet freedoms that has since escalated. Initially monitoring the Russian state internet blacklist, RKS has since expanded its remit to digital literacy work, online privacy and security workshops, advocacy campaigns for internet freedom and digital rights, and even offering legal assistance to Russian citizens prosecuted for internet activity.

I collected publicly available Russian-language activity reports from the official websites of the two organisations (https://rkn.gov.ru and https://roskomsvoboda.org), published between the start of 2015 and the start of 2019, a period of turbulent change in Russia's digital society and its governance. These reports (annual in the case of RKN, monthly in the case of RKS) represent key issues and activity performed or overseen by these actors in conjunction with their work. As these reports are regular, structured and explicitly aimed at disclosure for public consumption, they present a useful source of discourse about issues related to digital rights and privacy more specifically. For each organisation, I also collected the text from their 'About' or 'Mission' sections to capture how each organisation articulates its mission and objectives in the context of their work. Sampling their discourses in this way allows to capture fairly recent, but also regular and well-structured discourse relating to digital rights, communication, and information, and to locate any references to privacy therein. The discursive representations of privacy stemming from the analysis of these text corpora can then be connected to specific activity, showing how the competing politics of privacy shape state regulations, policy interventions, and activist efforts.

I collated the texts collected from each source into two text corpora. The resulting corpora contain 157,912 words (RKN) and 158,905 words (RKS), respectively. The RKN corpus contains text from five annual reports (154,584 words) and text from the 'About' page of RKN's website (3,328 words). The RKS corpus contains text from 54 monthly reports (158,743 words) and text from the 'Our Mission' page of RKS's website (162 words). I then used AntConc (Anthony, 2019), a freeware tool for conducting corpus linguistics and concordance analysis on large volumes of text, and specifically its 'Concordance' tool. A concordance is a commonly used display format in corpus linguistics similar to a table that shows instances of a selection of words in their context. I focused on concordances of specific words commonly used in privacy discourses—in this case the lemmas 'privacy' (*приватность* [privatnost], noun), 'private' (*приватный* [privatnyy] or *частный* [chastnyy], adjective), and 'personal' (*персональный* [personalnyy] or *личный* [lichnyy], adjective)—to uncover the semantic context in which they are most commonly used by each actor. Lemmas were used in order to capture all possible word endings and word forms in Russian.

AntConc has been used previously in communications, media, and policy research outside of corpus linguistics (e.g., Baker & McEnery, 2015; Fairclough, 2016; Lokot & Diakopoulos, 2016). Likewise, privacy and surveillance studies have often relied on discourse analysis to capture how public debates around privacy norms develop (e.g., Cichy & Salge, 2015; Möllers & Hälterlein, 2013). While the use of corpora in discourse analysis is well-documented (e.g., Baker, 2006), in this study a corpus linguistics tool was used primarily in order to reveal how privacy is discursively constructed by each organisation and how these discourses around privacy diverge. The frequency of specific words in this context was of less importance than the discourses that emerged around the privacy-related keywords in the RKN and RKS corpora. Therefore, though raw and relative frequencies for key terms are provided throughout, the analysis in this study is mostly qualitative in nature and examines the semantic fields (Fairclough, 2016) associated with the occurrence of privacy-related keywords in each corpus via their clusters, collocates, and concordances. Relevant examples from the text corpora provided in the article have been translated into English by the author.

## 4. Findings: Competing Discursive Constructions of Privacy

The raw ($F_O$) and relative (normalised, $F_N$) frequencies of the privacy-related keywords (lemmas) in both text corpora are presented in Table 1.

### *4.1. RKN*

A key observation from the RKN corpus is that the state regulator never once uses the more modern Russian term 'privacy' (*приватность*)—instead, the term of choice is the more commonly used 'private life' (*частная жизнь* [chastnaya zhyzn]; $F_O = 76$ per 157,912 words, $F_N = 4.812807133$), along with terms such as 'personal' or 'family' used to denote personal or private contexts. Another notable observation is the coupling of 'inviolability' (*неприкосновенность* [neprikosnovennost]) with the context of privacy and private information (collocation frequency with 'private' within five words to the left or right at $F_O = 16$ per 157,912 words, $F_N = 1.013222554$)—this is not surprising, as these terms are often co-located in Russian legal parlance in information- and privacy-related contexts. An example of such collocation can be found in RKN's 2017 annual report, where the state blocked website registry is described as: "A regulatory instrument unique to international law that allows to protect the rights of Russian citizens to inviolability of their private life, their personal and family secrecy" (RKN, 2018, author's translation).

The state regulator's public communications discuss privacy in a predominantly instrumental context, referring to the 'personal data' of individuals ($F_O = 599$ per 157,912 words, $F_N = 37.932519378$), but rarely discussing individuals as active agents exercising their rights or freedoms. The focus is overwhelmingly on what is being done to the individual/user, rather than on their own actions: i.e., their private life is protected (by the state), and their personal data is collected and stored (by the state or third parties).

In its 2015 annual report, RKN describes a state official from the President's Office speaking at an RKN committee meeting and stressing that: "The main priority for state oversight and protection of personal data should be…the provision of individual security without infringing on private life" (RKN, 2016, author's translation).

**Table 1.** Raw and relative keyword frequencies in the RKN and RKS text corpora.

| Keyword | RKN $F_O$ | RKN $F_N$ * | RKS $F_O$ | RKS $F_N$ * |
|---|---|---|---|---|
| Privacy | 0 per 157,912 | 0 | 29 per 158,905 | 1.824989774 |
| Private | 79 per 157,912 | 5.002786362 | 288 per 158,905 | 18.124036374 |
| Personal | 645 per 157,912 | 40.845534222 | 334 per 158,905 | 21.648154558 |

Note: * Relative frequency $F_N$ per 10,000 words.

These instances point to the preoccupation of the state with monitoring citizen online activity, establishing blanket digital surveillance, and ensuring ad-hoc access to personal information flows, while seeking to shield it from external actors.

Individual rights to privacy are framed in RKN's discourse as rights of 'personal data subjects,' reinforcing the instrumental context of state-controlled subjects generating data. In the RKN corpus, discourse related to 'defence' and 'protection' tends to be clustered together with 'personal' data of subjects and not with discussion of their individual privacy. For instance, in its 2018 annual report, RKN elaborates on practical and preventative measures implemented that year and, among other activities, boasts that: "The greatest number of preventative training events was held in the area of personal data protection—12,579 activities in total" (RKN, 2019, author's translation).

In a similar activity summary in the 2017 annual report, RKN reports that: "Greater attention was given to events aimed at school pupils and students in order to cultivate a culture of care with regard to their personal data" (RKN, 2018, author's translation).

This discursive instrumentalisation of privacy extends from protecting copyright and intellectual property to personal data to defending the interests of the Russian state in cyberspace. In all of these cases, the object being protected is either information or the state, and not the privacy of individuals.

The privacy-adjacent discourse around security and safety in the text corpus further confirms this: The RKN corpus clusters 'digital security' alongside 'personal data protection' and 'safe online behaviour'. The focus is on a secure and safe environment and data, as well as law and order, rather than on the individual and their privacy choices. In the 2018 report, the state regulator explicitly states: "In the context of the global transformation of the information world order, we see [our] main goal as ensuring security and protection for society and citizens from relevant cyberthreats" (RKN, 2019, author's translation).

Thus, individual privacy and privacy of personal data flows is predominantly contextualised by RKN as a matter of national security and presented as a function of the sovereign state retaining control over information and data of its 'subjects' to protect them against external threats.

### *4.2. RKS*

Unlike the state regulator, RKS readily uses both 'privacy' and 'private' (in both its traditional and modern forms) in its public discourse online (see Table 1 for frequencies). In the RKS corpus, these terms most commonly co-occur with 'rights' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O$ = 42 per 158,905 words, $F_N$ = 2.643088638), life (collocation frequency with 'privacy/private' within five words to the left or right at $F_O$ = 42 per 158,905 words, $F_N$ = 2.643088638), 'information' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O$ = 22 per 158,905 words, $F_N$ = 1.384475001), 'inviolability' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O$ = 10 per 158,905 words, $F_N$ = 0.629306819), 'data' (collocation frequency with *privacy/private* within five words to the left or right at $F_O$ = 10 per 158,905 words, $F_N$ = 0.629306819), and 'personal' (collocation frequency with 'privacy/private' within five words to the left or right at $F_O$ = 8 per 158,905 words, $F_N$ = 0.503445455), as well as in the context of protecting privacy and anonymity of users.

In its mission statement (RKS, 2019, author's translation), the digital rights organisation describes its aims in the following way: "Roskomsvoboda organises broad public campaigns and supports civic initiatives in favour of freedom of information and inviolability of the personal data of users."

In contrast to the state discourse, privacy in the discourse of digital rights activists is more closely connected to the rights and interests of individual citizens. Throughout the RKS corpus, RKS often refers to 'your privacy' (two-word cluster $F_O$ = 13 per 158,905 words, $F_N$ = 0.818098864) or 'their privacy' (two-word cluster $F_O$ = 9 per 158,905 words, $F_N$ = 0.566376137), drawing direct connections between the individual and their work. For instance, in a January 2015 monthly report, the organisation notes their legal director, Sarkis Darbinyan, participated in a seminar on internet regulation in the Russian city of Voronezh: "Darbinyan presented a short summary of technologies that help users, website owners and journalists circumvent the blocking of Internet resources and preserve their privacy online by using new digital rights such as the right to anonymity and encryption" (RKS, 2015a, author's translation).

The privacy-related discourse of RKS is more concerned with agency in the sense that privacy is presented as something the individual or the user can achieve or preserve, as opposed to something that the individuals are granted by some external power. In this regard, RKS regularly references specific tools that individual users can avail of to exercise and protect their privacy, including virtual private networks (VPNs), the TOR browser (a tool that camouflages users' IP addresses), and various encrypted communication options. In its June 2015 monthly report, RKS references a recent intervention discussing the advantages of using the TOR browser in the context of growing restrictions imposed by the Russian government on the online sphere: "We saw a sharp uptick in TOR browser use, because the new reality pushes people to search for new solutions so they can access their favourite websites. In addition, TOR can ensure your privacy online" (RKS, 2015b, author's translation).

Importantly, the RKS discourse links privacy to specific rights of networked citizens, such as anonymity, secrecy, unhindered distribution of information, access to digital networks, and encryption. In a public lecture on digital rights for students, trainee lawyers and civic activists in Moscow, held in September 2015 and mentioned in the monthly report for the same period, a representative for RKS underscored that:

> Protecting the rights and freedoms of a person in an online environment is just as important as in everyday life, and you should not forfeit your rights to privacy, security and freedom to obtain and disseminate information under any circumstances. (RKS, 2015c, author's translation)

In their reports, digital rights activists discuss examples of user activity on specific platforms, such as Telegram, and refer to personal data and user identification in the context of these cases. For instance, in December 2017 RKS reports on a new 'Battle for Telegram' campaign it launched in support of the Telegram messenger, which was facing pressure from the Russian government to share user information and encryption keys: "If we do not protect this internet service that cares about the privacy of our data today, Russian users may become an easy target for cybercriminals and illegal actions on the part of the state institutions" (RKS, 2017b, author's translation).

When discussing the need to protect individual privacy and personal data flows, RKS unambiguously points to the Russian state as the main threat against which privacy must be protected. In multiple instances, the activists critique new and upcoming internet regulations developed by the state, such as the 'anti-extremist' Yarovaya law (Luganskaya, 2017). As observed in the December 2016 monthly report summarising key developments in Russian internet regulation in 2016 (RKS, 2016b, author's translation), RKS experts see the Yarovaya law as "eradicating privacy by default" for Russian internet users. Thus, the notion of personal information security is presented in terms of what citizens can do to protect their privacy online, and how this individual agency is contested by the state as part of its national security discourse.

As an activist and advocacy organisation, RKS sees its mission as more than offering legal defence and technological solutions (such as their VPN Love project recommending verified VPN services). Crucially, activists also promote individual agency by asking the users to defend themselves from state surveillance and fight for their privacy. This is supported by RKS's own initiatives, such as the SAFE Project announced in January 2017 and aimed at educating the public about a range of anti-surveillance and privacy tools: "Roskomsvoboda is launching a new resource—Project SAFE—about self-defence tools for internet users to protect themselves from surveillance and intrusions into their personal data and correspondence" (RKS, 2017a, author's translation).

Privacy-related agency, the activists argue, can be achieved through increased public debate and digital literacy, and this aligns with their advocacy efforts aimed at giving the users more control over their information and online presence. These efforts include public documentation of state persecutions against internet users, disseminating detailed instructions on how to appeal internet-related charges, and developing practical tips on protecting oneself from digital surveillance. As RKS notes in its mission statement on its website: "Our aim is for every RuNet [Russian Internet] user to be able to defend their [digital] rights" (RKS, 2019, author's translation).

### *4.3. Privacy: Contextual, Relational, and Political*

In both the state regulator's and the digital rights activists' public online discourses, privacy is constructed as contextual, relational, and political. However, these articulations diverge greatly in terms of the normative foundations on which they are constructed. The discursive divergence also extends to how privacy is reflected and enacted by both the state and activists in terms of policy, regulations, and sanctions, as well as in terms of grassroots action, digital literacy efforts, and digital rights initiatives.

As a state institution, RKN interprets privacy of individual data and information flows predominantly in the context of Russia's national security and digital sovereignty concerns. In this almost geopolitical view, individuals are viewed not as independent agents empowered to protect their own private lives, but as 'personal data subjects' of the state, whose data require state protection, regulation, and control. This contextual interpretation of privacy is reflected in the Russian regulatory landscape over the past decade: Legislative acts such as the Yarovaya law (Luganskaya, 2017) and the internet sovereignty law (Lipman & Lokot, 2019) approach internet governance, online safety, privacy, and personal information as matters of national security, while the power to regulate and protect resides in the hands of state institutions. Privacy, therefore, emerges as a relational concept wherein the institutions of the state, be they telecom regulators such as RKN or law enforcement bodies, are involved in mediating and enabling individual private life, while also remaining constantly in control of personal data flows and in possession of access to individual data and metadata of Russian citizens. As the state and its institutions see themselves as granting privacy to citizens, they also conclude that they have the power and the right to grant or withhold privacy. This is reflected in the multiple instances of arbitrary requests for user data from social media platforms (Gadde, 2019; Lokot, 2016), alleged violations of privacy against opposition activists (Seddon, 2016), and the selective application of legal norms to persecute users for online expression (Mostovshchikov, 2015). This ongoing struggle for control over the field of privacy (with foreign governments, platforms, and users themselves) renders privacy as a clearly political issue for the Russian networked authoritarian state. However, the politics here is that of a hegemonic state that seeks to preserve the status quo and to retain its power over information and data flows at the cost of the individual agency of its citizens.

In contrast, digital rights activists at RKS view privacy in the context of digital rights and freedoms and discursively present it as a key individual right in the digital age. For RKS, privacy is a key expression of individual agency as it is something each person can achieve or protect if given the proper tools and knowledge. This is reflected in RKS's digital literacy initiatives such as Project SAFE (described in Section 4.2 above). The activists also construe of privacy as relational, but in a different sense: For them, the struggle is that of the individual user attempting to wrestle the privacy of their data and their personal security from the grasp of the state. This is why RKS and their allies launch and maintain grassroots campaigns in support of privacy-enabling platforms such as Telegram (Novaya Gazeta, 2017) or in defence of individuals persecuted by the state for using privacy and anonymity tools, such as Russian TOR relay node operator Dmitry Bogatov (Gilmour, 2017). Though privacy-enhancing technologies are seen as beneficial in terms of user agency in general, it is the state that is seen as the biggest threat in the conditions of Russia's networked authoritarianism. In this respect, RKS also intervenes in the development and implementation of internet and privacy regulations, submitting opinions on new initiatives it believes to threaten privacy such as facial recognition systems (Kornya, 2019) and contesting legal sanctions impinging on user privacy in court (RKS, 2020).

In the circumstances of diminishing space for free expression and genuine political participation, digital rights activists promote a political articulation of privacy as a crucial condition of individual freedom to exercise political agency and to renegotiate the balance of power—both power writ large and power over the private lives of individuals—with the dominant governing regime. The activist politics of privacy, therefore, is aimed at the transformation of the status quo and at bringing about change at the grassroots level.

## 5. Conclusion: Data Subjects vs. People's Data

This study examines the discursive representations of issues surrounding privacy by the Russian state internet regulator RKN and by digital activist group RKS, and uses this discursive analysis to highlight relevant concerns in the Russian public sphere with regard to technological systems and digitally-mediated practices related to flows of personal information. This study contributes to the existing scholarship on internet governance and digital rights and offers critical insights into how privacy politics informs the contestation of citizenship and, consequently, the distribution of power in different kinds of democratic systems, including hybrid regimes such as Russia. The study also makes a contribution to the scholarship on privacy politics in media and communications research by using corpus linguistics tools for privacy-related discourse analysis.

Though both the state telecom regulator and the activists construe privacy as contextual, relational, and political, their interpretations of privacy and their privacy politics diverge significantly. By examining the articulations of the concerns, norms and regulations around privacy by the state institutions and grassroots digital rights advocates, I show how the struggle for control over accessibility of private data and resistance against restrictions of personal data flows lead to two different concepts of the politics of privacy in Russia.

I find that the networked authoritarian Russian state sees its citizens as vulnerable data subjects with little agency, whose private identities and communications should be protected from 'foreign interference,' but must always remain visible and accessible to the state. On the other hand, Russian digital rights activists advocate for privacy as a human right and argue that technologies such as encryption and VPNs should be widely adopted by citizens to preserve their agency and protect their data and identities from the state. These tensions between interpretations of privacy by the Russian state and Russian citizens inform how privacy is negotiated as part of the ongoing political dissent and the struggle over divergent political visions of Russian society.

The differential understandings of how anonymity, secrecy, confidentiality, and control of personal data determine the distribution of power and agency in Russian public and political life shape the resulting politics of privacy in Russia, as reflected in the state's struggle for control over accessibility of private data and the grassroots resistance against restrictions of personal data flows. These divergent politics are reflected in privacy-related policing and control on the part of the state, and in privacy-related advocacy, activism, and digital literacy initiatives of activist groups. Amid the precarity of online expression and the struggle for control over personal data flows, the ongoing contestation of privacy-related power has implications for what kind of political future Russian citizens might anticipate: one where they are 'data subjects' at the mercy of a hegemonic state or one where their privacy enables greater political agency and allows them to refashion society towards a more equal, democratic, and rights-based vision.

Beyond Russian borders, many former Soviet states that Russia counts within its sphere of influence are closely watching the developments in internet governance and digital identity policies developed and contested in Russia. Further research by media and communication scholars focusing on Central and Eastern Europe should therefore examine the possible repressive or democratising impact of the discursively contested articulations of privacy politics in Russia on its neighbour states. Related research could also examine the overlaps and divergences of emergent privacy politics within EU states and within Russia, in light of the recent adoption of the General Data Protection Regulation and greater attention to personal data protection and privacy concerns.

## Acknowledgments

This article was made possible with support from the 2019–2020 Journal Publication Scheme of the Faculty of Humanities and Social Sciences, Dublin City University.

## Conflict of Interests

The author declares no conflict of interests.

## References

Anthony, L. AntConc (Version 3.5.8) [Computer software]. (2019). Tokyo: Waseda University. Retrieved from https://www.laurenceanthony.net/software

Baker, P. (2006). *Using corpora in discourse analysis*. London: Continuum.

Baker, P., & McEnery, T. (2015). Who benefits when discourse gets democratised? Analysing a Twitter corpus around the British Benefits Street debate. In P. Baker & T. McEnery (Eds.), *Corpora and discourse studies* (pp. 244–265). London: Palgrave Macmillan.

Boym, S. (1994). *Common places: Mythologies of everyday life in Russia*. Cambridge, MA: Harvard University Press.

Cichy, P., & Salge, T. (2015). The evolution of privacy norms: Mapping 35 years of technology-related privacy discourse, 1980–2014. In *Proceedings of the Thirty Sixth International Conference on Information Systems* (pp. 1–13), Fort Worth, TX: Association for Information Systems.

Fairclough, I. (2016). Evaluating policy as argument: The public debate over the first UK austerity budget. *Critical Discourse Studies*, *13*(1), 57–77.

Fairclough, N. (2013). Critical discourse analysis. In J. P. Gee & M. Handford (Eds.), *The Routledge handbook of discourse analysis* (pp. 9–20). Oxford: Routledge.

Gadde, V. (2019). Key data and insights from our 14th Twitter transparency report. *Twitter Blog.* Retrieved from https://blog.twitter.com/en_us/topics/company/2019/key-data-and-insights-from-our-14th-twitter-transparency-report.html

Gilmour, D. (2017, April 26). Russian Tor relay operator facing terrorism charges. *Daily Dot*. Retrieved from https://www.dailydot.com/debug/russian-tor-relay-operator-facing-terrorism-charges

Gorny, E. (2007). *The Russian internet: Between kitchen-table talks and the public sphere*. Boston, MA: Art Margins.

Greene, S. (2012). *How much can Russia really change? The durability of networked authoritarianism*. Washington, DC: PONARS Eurasia.

Kornya, A. (2019, October 6). Moskvichka prosit sud zapretit' raspoznavaniye lits gorodskoy sistemoy videonablyudeniya [Muscovite asks court to ban facial recognition by city CCTV system]. *Vedomosti*. Retrieved from https://www.vedomosti.ru/politics/articles/2019/10/06/812955-moskvichka-prosit-sud

Levontina, I., Shmelev, A., & Zaliznyak, A. (2017). *Konstanty i peremennye russkoy yazykovoy kartiny mira* [The constants and variables of Russian language world view]. Moscow: Litres.

Lipman, M., & Lokot, T. (2019). Disconnecting the Russian internet: Implications of the new "digital sovereignty" bill. *PONARS Eurasia.* Retrieved from http://www.ponarseurasia.org/point-counter/article/disconnecting-russian-internet-implications-new-digital-sovereignty-bill

Lokot, T. (2016, March 6). Twitter reports massive increase in Russian government's content removal requests. *Global Voices*. Retrieved from https://globalvoices.org/2016/03/06/twitter-reports-massive-increase-in-russian-governments-content-removal-requests

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.

Lokot, T., & Diakopoulos, N. (2016). News bots: Automating news and information dissemination on Twitter. *Digital Journalism*, *4*(6), 682–699.

Luganskaya, D. (2017, April 23). Open economy: Kak rossiyskiye vlasti budut kontrolirovat' internet. Tri osnovnykh sposoba [Open economy: How the Russian authorities will control the internet. Three main ways]. *Open Russia*. Retrieved from https://openrussia.org/notes/708721

MacKinnon, R. (2011). Liberation technology: China's "networked authoritarianism." *Journal of Democracy*, *22*(2), 32–46.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Dublin: Houghton Mifflin Harcourt.

Merzlikin, P. (2019, April 18). 'In a perfect world, we just wouldn't exist' How Roskomsvoboda became the primary force standing between the Russian government and Internet censorship. *Meduza*. Retrieved from https://meduza.io/en/feature/2019/04/19/in-a-perfect-world-we-just-wouldn-t-exist

Möller, J. E., & Nowak, J. (2018). Surveillance and privacy as emerging issues in communication and media studies: An introduction. *Mediatization Studies*, *2*, 7–15.

Möllers, N., & Hälterlein, J. (2013). Privacy issues in public discourse: The case of "smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research*, *26*(1/2), 57–70.

Mostovshchikov, E. (2015, February 9). 'There's no such thing as an accidental repost' How Russia punishes people for likes, retweets, and selfies. *Meduza*. Retrieved from https://meduza.io/en/feature/2015/02/09/there-s-no-such-thing-as-an-accidental-repost

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

Novaya Gazeta. (2017, December 21). V Rossii zapustili kampaniyu dlya podachi kollektivnoy zhaloby “Telegram protiv FSB” [“Telegram vs. FSB” campaign launched in Russia for collective appeal]. *Novaya Gazeta*. Retrieved from https://novayagazeta.ru/news/2017/12/21/138115-v-rossii-zapustili-kampaniyu-dlya-podachi-kollektivnoy-zhaloby-telegram-protiv-fsb

Roskomnadzor. (2016). *Publichnyy doklad za 2015 god* [2015 annual public report]. Moscow: Roskomnadzor. Retrieved from https://rkn.gov.ru/docs/docP_1485.pdf

Roskomnadzor. (2018). *Publichnyy doklad za 2017 god* [2017 annual public report]. Moscow: Roskomnadzor. Retrieved from https://rkn.gov.ru/docs/doc_2326.pdf

Roskomnadzor. (2019). *Publichnyy doklad za 2018 god* [2018 annual public report]. Moscow: Roskomnadzor. Retrieved from https://rkn.gov.ru/docs/doc_2406.pdf

Roskomsvoboda. (2015a). Roskomsvoboda prinyala uchastiye v seminare po pravovomu regulirovaniyu I problemam rasprostraneniya informatsii v Seti [Roskomsvoboda participates in seminar on legal regulation and issues of information distribution online]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/10202

Roskomsvoboda. (2015b). Master-klass Roskomsvobody: Internet I zakon. Prava, obyazannosti I otvetstvennost v onlayne [Roskomsvoboda master-class: Internet and the law. Rights, obligations and responsibilities online]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/11869

Roskomsvoboda. (2015c). Roskomsvoboda provela seminar dlya yuristov-volontyorov I aktivnykh grazhdan: Prava pol’zovatelya v Internete [Roskomsvoboda holds seminar for volunteer lawyers and active citizens: User rights on the internet]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/12894

Roskomsvoboda. (2016b). Itogi gosregulirovaniya interneta v Rossii v 2016 godu [Summary of state internet regulation in Russia in 2016]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/24592

Roskomsvoboda. (2017a). Proyekt SAFE: Zashchiti sebya ot slezhki [SAFE Project: Protect yourself from surveillance]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/24961

Roskomsvoboda. (2017b). Roskomsvoboda zapustila obshchestvennuyu kampaniyu “Bitva za Telegram” [Roskomsvoboda launches public campaign “Battle for Telegram”]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/34243

Roskomsvoboda. (2019). Proekty [Projects]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/projects

Roskomsvoboda. (2020). TgVPN i РосКомСвобода obzhaluyut deystviya rossiyskikh gosorganov v ESPCH [TgVPN and Roskomsvoboda to appeal Russian state institutions’ actions in ECHR]. *Roskomsvoboda*. Retrieved from https://roskomsvoboda.org/54384

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, *10*, 2221–2237.

Seddon, M. (2016, May 6). Activists say Russian telecoms group hacked Telegram accounts. *Financial Times*. Retrieved from https://www.ft.com/content/74d5ce00-12dd-11e6-839f-2922947098f0

Soldatov, A., & Borogan, I. (2013). Russia’s surveillance state. *World Policy Journal*, *30*(3), 23–30.

Russian Federation. (2006). *Federalnyy zakon “O personal’nykh dannykh”* [Federal law “On personal data”] (N 152-FZ). Moscow: Russian Federation. Retrieved from https://www.consultant.ru/document/cons_doc_LAW_61801

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society*, *3*(1), 1–13.

Turovsky, D. (2015, August 13). This is how Russian Internet censorship works. *Meduza*. Retrieved from https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Westin, A. F. (2015). *Privacy and freedom*. New York, NY: IG Publishing.

## About the Author

**Tetyana Lokot** is an Assistant Professor at the School of Communications, Dublin City University. She has been researching activism, protest, internet governance, and censorship on the Cyrillic web for over a decade. Tetyana’s work has been published in *Information, Communication and Society*, *Surveillance and Society*, *International Journal of Communication*, and *Digital Journalism*, and presented at international academic conferences. She is currently working on a book about protest and digital media in Ukraine and Russia.

**Media and Communication (ISSN: 2183-2439)**

*Media and Communication* is an international open access journal dedicated to a wide variety of basic and applied research in communication and its related fields. It aims at providing a research forum on the social and cultural relevance of media and communication processes.

www.cogitatiopress.com/mediaandcommunication

COGITATIO