MEDIATIZATION STUDIES 1/2018 DOI: 10.17951/ms.2018.1.2.7-15

JOHANNA E. MÖLLER

Department of Communication, Johannes Gutenberg University Mainz, Germany

johanna.moeller@uni-mainz.de

JAKUB NOWAK

Department of Journalism, Maria Curie-Skłodowska University in Lublin, Poland

jakub.nowak@poczta.umcs.lublin.pl

Surveillance and privacy as emerging issues in communication and media studies. An introduction

Surveillance and privacy are two closely related issues that continue to move into the heart of communication and media studies. This special issue joins contributions which illustrate that surveillance and privacy play multiple roles in mediated communication. So far, these have been predominantly investigated by researchers with an interdisciplinary approach. Data collection and analysis, for instance, are significant in sociology-related surveillance studies (Lyon 2002). This issue is regularly covered by communication and media researchers dealing with political media activism and mobilization (Hintz et al. 2019). With reference to psychology, privacy is discussed in the light of knowledge and the actions related to data collection and information boundary management (Trepte et al. 2017; Trepte 2016). In a similar vein, the privacy of teenagers and young adults is a specific concern (Balleys, Coll 2017; Marwick, boyd 2014). As yet, currently, privacy and surveillance related issues constantly gain importance they spread across the field of communication and media studies.

With contemporary mediatization and datafication of societies, surveillance and privacy play an increasing role across all communication and media subdisciplines, and tend to form a core theme in the field. Considerations related to data collection and analysis, on the one hand, and managing individual and organizational information boundaries, on the other, are subject to mundane, everyday media practices. Both relate to customer data, such as that provided as part of offline and online shopping

or with car tracking data. Another key concern is social media communication, as there is increasing awareness and knowledge of the massive collection of data by large technology companies. Beyond that, privacy plays a key role as an educational issue, such as in the avoidance of bullying or other forms of private data exposure. Being a member of digital societies implies a certain ability of managing information and can lead to a loss of control over one's personal data. Absolute privacy, yet, would be equivalent to social isolation.

Beyond this mundane and everyday level of dealing with the collection and analysis of data, traditional questions from the field of communication and media research now increasingly link to the subjects of surveillance and privacy. Political communication research, to mention one example, investigates the collection and uses of voter data. Several studies point to the resurgence of door-to-door canvassing and face-to-face campaigning emerging from increased options for data analysis (i.e. Hillygus, Shields 2009; Kruschinski, Haller 2017). In countries with liberal data regulation, combining geo-locational and content data allows swing voters to be addressed directly. This has considerable implications for democracies as new inequalities emerge. Distinguishing the to-be-convinced as "useful" and the taken-for-granted as "useless", voters can increase the effects of silencing viewpoints and the needs of the latter. Moreover, following studies on Facebook's effective influence on participation in national elections (i.e. Bond et al. 2012; Sifry 2014), the methods of processing users' data by commercial companies has become one of the key issues for digitized democracies.

Second, in the wake of increased data observation and analysis potentials, journalism research also addresses emerging inquiries. Beside the issues rising during the past few years, such as the "normalization of surveillance" (Wahl-Jorgensen et al. 2017), whistleblowing practices (Kunelius et al. 2017) and privacy in media coverage (von Pape et al. 2017), new modes of journalism are shaping scholarly debates (Kramp, Loosen 2017). While data journalism was celebrated for its potential objectivity and as a revolutionizing form of media coverage, current research has tended to partially withdraw from these high expectations (Wahl-Jorgensen 2017). Loosen et al. (2017) have proven that data journalism relies on (publicly) available data instead of establishing its own, which is very likely to lead to biased coverage. That is, data journalists are trapped in conflicts between collecting sensitive data for differentiated media coverage and the respect for the individuals' rights. Issues of surveillance and privacy thus redefine contemporary journalism.

Research in the area of media industries, as a third and final example, deals with agents that profit from the need to collect, analyze and protect individual data. Business models arise that are based both on data collection and analysis (Fuchs 2011) as well as on privacy protection. Recent discussions on Facebook's surveillance and privacy practices illustrate that both are often intimately intertwined. Data protection activists recently revealed that Facebook, under the pretext of privacy protection, misuses two factor authentication to collect and use people's individual mobile phone

numbers for business purposes (Whittaker 2019). From a political economy perspective, data is a resource unequally distributed among agents. While large technology platforms use de-centralized platforms to collect all kinds of data (Helmond, 2015), legacy media companies dispose of significantly less access to information on their users and, as such, experience considerable competitive disadvantages (Möller, von Rimscha 2017). Practices of data collection and protection thus have a significant impact on imbalances in the media market.

These three examples from the field of communication and media studies underline the contextual, relational and often political character of both surveillance and privacy, as put forward by the contributors to this volume. First, and regarding contextual aspects, following Helen Nissenbaum's (2010) understanding of contextual integrity, surveillance as well as privacy must consider that they must be conceptualized and reconceptualized with a view to every specific context. Nissenbaum develops her argument with the intent to develop normative concepts of privacy. In her view, privacy needs to be constantly reconsidered and redefined. Irrespective of whether it concerns individuals, groups or institutions, privacy is defined separately for such different contexts as education, consumption and economics. Not least, the cultures of privacy can differ considerably. These considerations are precondition for Nissenbaum's argument against public surveillance. While privacy is able to consider contextual specifics, surveillance is not, as it absorbs all data: "public surveillance violates the right to privacy because it violates contextual integrity" (Nissenbaum 2004, p. 101). Nissenbaum has inspired normative approaches in the field, such as that of data justice (Dencik et al. 2018), but her insights can be applied beyond. Trepte et al. (2017), in applying privacy calculus, have found that privacy clearly differs across cultures.

Surveillance and privacy are, second, relational. Both are not realized by individuals, but by individuals within societies. Among the individual approaches to privacy, most prominent is Westin (2015, p. 67), who defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Following Westin, the privacy calculus approach deals with privacy as the "process of boundary management and the strategies used by individuals to regulate access to the self" (Trepte et al. 2017, p. 2). It implies that the disclosure of and access to private information occurs after a calculation of the costs and benefits. The privacy calculus is relational, as agents, despite their awareness of privacy risks, accept partial violations of data security to prevent loss of their communicative networks. Using the example of teenage privacy, Balleys and Coll (2017) argue that private information can be used as a resource that is actively shared with those trusted (see also Livingstone 2008). In terms of privacy violation, Marwick and boyd (2014) reveal how within Social Network Sites the group settings trump individual security settings. Surveillance, in turn, profits from this relational data.

Finally, emerging publications in the field of communication and media studies point to the often political or participatory character of surveillance and privacy. While

the political character of surveillance has become highly visible since the Snowden revelations (Kunelius et al. 2017), digital media increasingly bring to the fore the more subtle political dimensions of privacy. The privacy behavior of individuals increasingly affects that of others, so that joint or societal solutions need to be found. Beyond that, voicing political positions in the web, as for instance in authoritarian contexts, can increase demands for data security (Lokot 2018). In presenting a study on the media practices of Polish and German privacy activists, we have referred to the example of an activist who publicly used information on his family's exposure to a police house search (and how it affected his children's mental health) to raise awareness of surveillance issues (Nowak, Möller 2018).

Following these basic considerations, the collection of academic texts in this volume addresses emerging communication and media perspectives on surveillance and privacy. In this sense, surveillance is understood as the massive and often undirected collection of any kind of information, by and on individuals, groups or organizations. Privacy, in contrast, relates to the ability to reflect on the potential effects of these analyses on societies and individuals, and the ability and right to take action to protect individual, organizational and collective information boundaries. This includes attempts to illustrate the contextual, relational and often political character of surveillance and privacy. Consequently, this volume explores relatively diverse societal constellations of surveillance that require specific concepts of privacy. The following contributions repeatedly show that, and how, individuals and organizations cope with managing these complex and interwoven demands, and the challenges of data collection, analysis and protection.

In particular, *Helena Atteneder* and *Bernhard Collini-Nocker* link ideas from communication and media studies with know-how from information sciences. In their article, they focus on privacy attitudes and practices regarding geo-locational data, where the specifics derive from being largely invisible to the users. While those with higher education know about and use the opt-out options for sharing locations, there remains a whole bundle of shared data remaining invisible. This research touches on the subtle tensions and conflicts between a knowledge of corporate geo-locational surveillance and pro-active measures against it. Atteneder and Collini-Nocker combine a quasi-experimental setting and an online questionnaire to investigate the awareness and practices related to geo-locational data. They shed light on distinct privacy practices, where sharing geo-locational data is linked to contexts and networks. When confronted with the amount of invisible data being tracked, the participants discovered that while they generally took measures to protect the visible data, none of them was aware that only abstinence from geomedia could protect them from massively sharing geo-data. Both findings, the authors conclude, challenge the privacy paradox.

Similarly, *Grzegorz Ptaszek* investigates the relation of awareness, knowledge and privacy practices among well-educated Polish adolescents. Reaching for the concept of surveillance capitalism, he conducted a questionnaire-based study to identify young

digital technology users' attitudes towards how their personal data is gathered and processed for commercial reasons, and what practices these users perform to protect their online privacies. Ptaszek's study results are complementary to those of Attenender and Collini-Nocker: having only a moderate knowledge of particular corporate surveillance practices, young adults tend to secure their privacy more when provided with more information on the potential and actual processes of data harvesting by hi-tech market agents. Despite their awareness of and active engagement in protecting their personal data against misuse by others, they hardly ever perform activities to lower the associated risks. The potential problem of having one's privacy violated by data-processing companies seems to be too abstract and demanding for the many activities requiring greater technical competence.

Focusing more directly on various practices of surveillance evasion while underlining the inherently political nature of the practices in question, *Sven Braun* and *Anne-Marie Oostveen* take a closer look at the now mundane and culturally obvious technology and practices of emailing. In particular, they are interested in the sociopolitical contextualization of Pretty Good Privacy (PGP) – the most popular encryption software for email privacy protection since its origin in 1991. The study reveals that PGP encryption is far from being a mass or universal privacy protection technology. Only a relatively small homogeneous population of mainly Western, technically skilled, and moderately politically active males uses it for their informational self-management. This contribution joins numerous other issues, not only those covered in this volume, which shed light on the limits of privacy protection-oriented practices. Braun and Oostveen offer two views on these limitations. As PGP, similar to other encryption technologies, requires particular technical skills, a first view emphasizes the knowledge, awareness, skills and thus the citizens' political and cultural capital. An alternative perspective takes into account the different levels of convenience of digital technological tools. Are they easy to learn and use? In line with Atteneder, Collini-Nocker and Ptaszek, Braun and Oostveen show how privacy and surveillance comprise a field where technology, markets, politics and people's everyday practices intersect. Here even the poor usability of a given privacy protection solution becomes political, as it may imply or lead to significant biases.

Another paper exploring the deliberate practices of surveillance evasion is authored by *Mareile Kaufmann*. In her qualitative interview study, she explores the practices and purposes of hacking online surveillance. She describes hacking, understood broadly as practices related to re-appropriating communication standards, as a process of redefining what is seen and not seen in the context of online surveillance. Kaufmann develops her argument using critical theory's repository of cultural studies and applies Michel de Certeau's concept, tactics of everyday life, "moments of analytical creativity and reflection, instances of pleasure and play, affective encounters, identity work and forms of communication". Based on her qualitative interviews with hackers, she argues that hacking is a political culture that produces "impacts and artifacts", like manifestos, games, publications, and agreements – all designed to support legal and

well-established structures or to evade, transgress or oppose them. Hacking with the purpose of avoiding surveillance is, therefore, not necessarily a protectional, but rather a playful practice in the first place. It can be a moment of creative reflection and part of individual identity-building processes, as "hacking is never just resistance. Here, play means both: playing systems and playing with systems". However, this seems not to contradict its political nature. This also agrees with Braun and Oostveen's study, which shows that although PGP users may not be overly politically active, one third of the respondents admitted they started using PGP as a counter-reaction to government actions, such as surveillance.

The next two contributions explore a different aspect of the cultural and political status of digital technology; namely its discursive definition constructed in legacy media coverage. In particular, both papers analyze German public discourse on surveillance, data security and encryption. In their case study, *Florian Meißner* and *Gerret von Nordheim* seek to identify various facets of news reporting on surveillance, privacy and data security in the German quality newspaper, Süddeutsche Zeitung. Interested especially in how various risks in this context are depicted, they specify three key themes that emerge. The first theme refers to the violation of privacy norms by both state and private commercial agents. A second theme connects surveillance activities and (legitimate and illegitimate) power and law enforcement. The third theme refers to datafication and comprises coverage of both the potential risks and benefits of the increasing amount of data nowadays, and the political, economic and cultural implication of this trend. What is especially interesting here is that, despite the common belief that digital technology has been de-mystified since the Snowden leaks, the analyzed media coverage of issues concerning surveillance, privacy and data security has recently become even more affirmative and less focused on the potential risks. These increasingly positive and normative evaluations, the authors argue, may indicate a discursive shift towards the normalization of surveillance and data collection even in Germany, which is a liberal democracy-based society with a strong privacy protection tradition.

This paper is followed by *Linda Monsees*' complementary contribution. Monsees also examines German debates on encryption and the broader security discourse. Her research question is how encryption has been constructed as a political issue. Monsees' empirical material consists initially of legacy media coverage in two major German newspapers, Süddeutsche Zeitung and Frankfurter Allgemeine Zeitung, representing popular journalistic voices from liberal and conservative debates. Secondly, Monsees examines the statements of experts in public debates on these themes. Her results can be read as supplementary not only to Meißner's and von Nordheim's contribution, but to the all papers in the volume. Monsees careful analysis shows how encryption technology unfolds its ambiguous political meaning in and by discourse. Encryption is neither good nor bad, it can be obscure and protect, and thus relates to the complex tensions between security and self-determination in a digital age. The technology in question may form an obstacle for law-enforcement when encryption becomes

restrictive or as a means to protect governmental secrets. Security and encryption, as Monsees argues, is mostly discussed regarding the inherent risks, uncertainty, and complexities. Further, she shows that surveillance and encryption refer to specific historical and cultural contexts. Germany's experience with the Nazi dictatorship, Monsees argues, resulted in negative connotations about encryption against a background of potential state surveillance. Consequently, potential commercial threats to users' private data gain less discursive attention. Here Monsees' results go in line with the normalization argument explicated by Meißner and von Nordheim.

In the final contribution, *Piotr Celiński* focuses on the problem of how media technology is increasingly interwoven with people's bodies and tied to the processes of data collection and analysis. Celiński's theoretical essay on biosurveillance and biocontrol comprises a narrative about how surveillance, understood as a technology, a process, and, of course, a means of power, unfolds to become increasingly embedded in individuals' bodies. Celiński provides numerous examples illustrating the political topicality of this issue. Digital technology, he argues, becomes literally visceral to map the individuals' bodies, following the representational logic of traditional surveillance media. In this provocative piece, Celiński uses the repository of mediation theory in order to explain how the symbolic power of technological developments in the field of communication may transform our ways of sensing, perceiving and understanding the world around us. This process, he argues, radically redefines human subjectivity. Media, previously based on symbolic messages and physically distanced mediations, now shapes into direct, substantial actions impacting on personalities. What was symbolic and remote, and therefore relatively safe, has the potential to transform into direct material connections and transfers that bypass our senses, minds and conscious awareness. Michel Foucault has put forward the idea that potential control can always be the *actual* one, as it implies a promise of exercised power. Against this background, this cultural grammar of potential-thus-actual control can be read as the lowest common denominator of all the contributions in this volume.

Overall, this volume explores the contextual, relational and often political nature of surveillance and privacy. The papers show that there is more than one understanding of surveillance, as well as multiple approaches to privacy. While communication and media scholars, for instance, emphasize the critical perspectives on surveillance, content analyses bring to the fore that political discourse strongly contributes to positive or neutral views on the collection and analysis of data. Privacy, in particular, reveals its relational character when considering that socio-communicative networks regularly outdo surveillance awareness and digital technology skills. Finally, and fascinatingly, the contributions offer insights into the political character of surveillance and privacy. Often the political appears to emerge in passing, when considering hackers' practices or users of encryption technologies. While altogether these are but single contributions in a growing field of communication and media research, we still hope to have pursued some worthwhile ideas and thoughts.

* * *

This workshop was part of a larger Polish-German cooperation, brought into life by Jakub Nowak and Johanna E. Möller. Applying a cross-border comparative perspective, this initiative forwards various research projects under the thematic umbrella of privacy and media practices. Today, surveillance and privacy call for media practices having a potentially universal character as digital networks and companies can easily cross borders. Any surveillance or privacy policy, civic privacy strategy or even individual information boundary management requires cross-country and cross-cultural perspectives. Shared historical experiences with surveillance can shape privacy cultures and, consequently, technologies.

Both, this volume of "Mediatization Studies" and the workshop in Lublin, were generously supported by the Polish-German Foundation for Science as activities within the research project "Surveillance and Privacy in the Digital Age". Hereby, we want to express our gratitude to the Foundation and the anonymous reviewers of our project for their support and trust. We also like to explicitly thank the numerous reviewers for their engagement with reading and re-reading the contributions and their provision of extensive and helpful feedback. Not least, we thank the editors of "Mediatization Studies" for the trust they placed in us. Without their support this thematic volume would not be possible.

References

Balleys C., Coll S. (2017). Being publicly intimate: Teenagers managing online privacy. *Media, Culture & Society*, Vol. 39(6), pp. 885–901.

Bond R. M., Fariss C. J., Jones J. J., Kramer A. D. I., Marlow C., Settle J. E., Fowler J. H. (2012). A 61-million-person experiment in social influence and political mobilization, *Nature*, Vol. 489, pp. 295–298.

Dencik L., Jansen F., Metcalfe, P. (2018). A conceptual framework for approaching social justice in an age of datafication, DATAJUSTICE project, https://datajusticeproject.net/2018/08/30/a-conceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/, 01.02.2019.

Fuchs C. (2011). The Political Economy of Privacy on Facebook. *Television & New Media*, Vol. 13(2), pp. 139–159.

Helmond A. (2015). The platformization of the web: Making web data platform ready. *Social Media + Society*, Vol. 1(2), pp. 1–11.

Hillygus D. S., Shields T. G. (2009). *The Persuadable Voter. Wedge Issues in Presidential Campaigns*. Princeton University Press: Princeton.

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

Kramp L., Loosen W. (2017). *The transformation of journalism: from changing newsroom cultures to a new communicative orientation?* In A. Hepp, U. Hasebrink, A. Breiter (Eds.), *Communicative Figurations: Rethinking mediatized transformations*, Palgrave Macmillan: Basingstoke. pp. 205–239.

Kruschinski. S., Haller A. (2017). Restrictions on data-driven political micro-targeting in Germany. *Internet Policy Review*, Vol. 6(4), pp. 1–23.

Kunelius R., Heikkilä H., Russell A., Yagodin D. (Eds.). (2017). *Journalism and the NSA Revelations: Privacy, security, and the press*. I.B. Tauris: London.

Livingstone S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, Vol. 10(3), 393–411.

Lokot T. (2018). Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices. *Surveillance & Society*, Vol. 16 (3), 332–346.

Loosen W., Reimer J.; De Silva-Schmidt F. (2017). *Data-Driven Reporting – an On-Going (R) Evolution? A Longitudinal Analysis of Projects Nominated for the Data Journalism Awards 2013–2015*. Working Paper Series Hans-Bredow-Institut No. 41.

Lyon D. (2002). *Surveillance society: Monitoring everyday life* (Repr). *Issues in society*. Open Uniersity Press: Buckingham.

Marwick A. E., boyd d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, Vol. 16(7), pp. 1051–1067.

Möller J., von Rimscha M. B. (2017). (De)Centralization of the Global Informational Ecosystem. *Media and Communication*, Vol. 5(3), pp. 37–48.

Nissenbaum H. (2004): Privacy as contextual integrity. *Washington Law Review*, Vol. 79(1), pp. 101–139.

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

Nowak J., Möller J. E. (2018, November). *Don't hate the media. Act on media.*, Paper presented at the 7th ECREA Conference, Lugano, Switzerland.

Sifry M. *Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012*, Mother Jones, http://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout, 31.10.2018.

Trepte S. (2016). *The paradoxes of online privacy*. In M. Walrave, K. Ponnet, E. Vanderhoven, J. Haers, B. Segaert (Eds.), *Youth 2.0: Social media and adolescence. Connecting, Sharing and Empowering*, Springer International Publishing: Cham, pp. 103–115.

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*, Vol. 3(1), pp. 1–13.

Von Pape T., Trepte S., Mothes C. (2017). Privacy by disaster? Press coverage of privacy and digital technology. *European Journal of Communication*, Vol. 32(3), pp. 189–207.

Wahl-Jorgensen K. (2017). *A manifesto of failure for digital journalism*. In P. J. Boczkowski, C. W. Anderson (Eds.), *Remaking the News: Essays on the Future of Journalism Scholarship in the Digital Age, Inside Technology*, MIT Press, Cambrdige MA, pp. 251–266.

Wahl-Jorgensen K., Bennett L., Taylor G. (2017). The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of Communication*, Vol. 11, pp. 740–762.

Westin A. F. (2015). *Privacy and Freedom*. IG Publishing: New York.

Whittaker Z. *Facebook won't let you opt out of its phone number 'look up' setting*, Techcrunch, https://techcrunch.com/2019/03/03/facebook-phone-number-look-up/?guccounter=1&guce_referrer_us=aHR0cHM6Ly9uZXR6cG9saXRpay5vcmcvMjAxOS9mYWNlYm9vay-1taXNzYnJhdWNodC1oYW5keW51bW1lcm4tenUtd2VyYmV6d2Vja2VuLw&guce_referrer_cs=qtabV8dO1eMJbuNvjSOyJQ, 03.03.2019.