ORIGINAL ARTICLE

DOI: 10.51480/1899-5101.17.4(38).637

Doing Privacy: Exploring the Limits of Self-Determination

Jakub Nowak
0000-0002-5841-4404
Maria Curie Skłodowska Curie University, Poland

Johanna E. Möller
0000-0003-4377-2206
TU Dresden University of Technology, Germany

Abstract: Acknowledging the notoriously 'incomplete' nature of privacy has little effect on the considerable expectations the notion implies. Self-determined privacy points to reflexivity, critical practice and tech literacy. While privacy scholarship illustrates those points and explains how agents constantly fail in meeting these expectations, we ask the inverse question. What are the limits of privacy? Interviewing Polish and German activists who engage in privacy-conscious social and professional relations, this qualitative study strives to understand how self-determined privacy is realized. Focusing on how individuals shape their privacies as social agents, including the motivations and contexts of their practices, our insights serve as a case study highlighting the challenges of realizing the everyday endeavor of privacy in datafied environments.

Keywords: privacy, media practice, practice theory, activism, relational privacy

INTRODUCTION

In contemporary societies, the ability to shape privacy in a self-determined fashion gains increasing importance. Digitalization and datafication transform nearly everything, from relations or discourses to business models or politics. These transformations offer challenges and opportunities for individual privacy with surveillance as a problematic business model, practice, and norm (Lyon 2018; Zuboff, 2019) having impact on regular consumers and citizens.

Although self-determination is a key variable in this context, in datafied societies, people do not have equal opportunities to shape their own privacy. Even when considering that digital platforms' users can hardly avoid surveillance,

individuals do not seem to explore either their potentials for data security or alternative media use and their willingness to renegotiate privacy arrangements and thus shape their privacies in a more self-determined fashion. Awareness of the risks of privacy is a necessary precondition and the skills to reflect on media and technology as well as the ability to use and shape them are equally important (Büchi et al., 2017).

While research offers multiple insights into how individuals fail to cope with privacy challenges, there is a need to research the general limits of privacy in datafied societies.

Acknowledging that these limits exist, we focus on those agents who approach privacy as both crucial and prone to violation, and thus, would shape their communicative environment as needed. This paper presents a qualitative interview study with privacy experts, activists, and educators, analyzing their everyday privacy routines and challenges. We ask, where are the limits of self-determined privacy among agents who describe themselves as being privacy-savvy? How do they approach their privacies and what characterizes their activities? Answering these questions enables us to reconstruct broad and diverse repertoires of privacy-oriented media practices, which individuals who approach privacy as important and vulnerable perform. The answers also shed more light on the broader and still underdeveloped issue of the performance and limits of political agency in increasingly datafied online environments.

PRIVACY AS EVERYDAY MEDIA PRACTICES

Whereas research has traditionally focused on privacy as an individual problem, researchers have recently explored the collective aspects of privacy related self-determination. Scholars conceptualize privacy as 'doing' via complex repertoires of media practices, which acknowledge the ambivalent and contradictory nature of the phenomenon and position it in everyday media routines that are reflexive, contextual and inherently tied to activities of others.

FROM INDIVIDUAL TO RELATIONAL PRIVACY

Communication and media studies have a tradition of researching privacy as an individual challenge (see for overview Möller, 2024a). The privacy paradox—concerned with gaps between consciousness and risky practices, figures prominently in this tradition (Barnes, 2006). Understanding privacy as a strategy of individual control follows Westin's (2003) influential idea to understand it "as the claim of an individual to determine what information about himself or

herself should be known to others" (p. 431). Communication studies have further developed this perspective (Dienlin & Metzger, 2016; Trepte, 2021).

This approach that views privacy as an individual problem has been criticized as being an advocate of a liberal tradition that overlooks constraints caused by infrastructural injustices and imbalances (Gstrein & Beaulieu, 2022). The criticism is that this obfuscates views on digital platform societies while transferring liability for online outcomes onto end users (Sevignani, 2015). This also echoes the basic ideas of science and technology studies (Nahuis & van Lente, 2008) and critical cultural studies (Gillespie, 2010).

Limiting privacy debates to users' liability, though, would omit another important strand that sees privacy as mundane media-related practices. Practice-based approaches consider privacy as everyday routines in multiple social relations (Nissenbaum, 2009; Marwick & boyd, 2014; Möller, 2024b). Researchers in this field ask questions such as, what do users do (e.g. with media, technology, in relation to others…) when realizing privacies? Which meaning do they imply? Marwick and boyd's (2014) study on teenage privacy practices on Facebook, was an important initial step, which led to a corpus of similar studies (Balleys & Coll, 2017; Kumar et al., 2020).

SELF-DETERMINED PRIVACY

In users' self-determination, individualist privacy studies have researched relations between skills and practices. Traditionally, knowledge and consciousness related to risks have been promising variables that determine autonomous privacy. Privacy literacy, with its diverse reflexive and practical implications, plays a major role (Masur, 2020). In their everyday media-oriented practices, people construct a range of privacies for specific strategic purposes (Nippert-Eng, 2010). Individuals use several criteria to decide on how to do privacy, including 'who is involved' and 'what social roles are being played'; and the personal normative evaluation of 'fairness' of a particular situation or even common convenience (Kennedy et al., 2017).

Considering privacy as a process that emerges through practice, other researchers shift their focus to relations. Pink et al. (2018) show how household members share privacy care work, build regimes of "friendly surveillance" and shape each other's attitudes and practices. Other studies provide insights into how education can make a difference in this regard (Tiemann et al., 2021). Kumar et al., (2020) observed learning effects when children discuss privacy norms instead of rules and thus understand their active role in shaping their privacies.

Insights from privacy education hint at the importance of discourses shaping privacy perceptions. Scholars often use this argument, yet rarely discuss it in a more explicit fashion (Lyon 2018). Kumar et al. (2020) show how norms and trust

related to confidentiality play a key role in developing self-determined privacy. Similarly, "people who experience more perceived control over limited aspects of privacy sometimes respond by revealing more information, to the point where they end up more vulnerable" (Brandimarte et al., 2013, p. 340), which suggests that users can misuse discourses (Banks, 2015) and misplace trust (Brandimarte et al., 2013). Consequently, however users talk about privacy it has an impact.

Finally, infrastructures affect how privacy is performed. We find considerable overlaps with IT literature, focusing on how the design of infrastructures can foster reflexivity or decision-making. Dourish et al. (2004) argue that information sharing and hiding are two sides of a 'privacy' coin, yet do not appear on equal terms in user interfaces. Gallagher et al. (2017) suggest improvements of encryption technologies to secure online behavior. In the broader context, datafication driven by "the technical ability to turn increasing amounts of social activity and human behavior into data points that can be tracked, collected and analysed" (Hintz et al., 2019, p. 42), poses tremendous challenges to privacy as self-determination practices. To answer this challenge on the level of theory and research design, we introduce the concept of privacy as media practice in the next section.

PRIVACY AS (STRATEGIC) MEDIA PRACTICE

Understanding privacy as communication and media practices follows the initial research by Couldry (2004) on media practices as meaningful ways people do things with media. The underlying aim is to understand the role of media in contemporary societies, which resonates with a shift of focus on social phenomena and avoiding a centralization of the media. Based on the premise that any realm of everyday meaningful action is "mediatized" (Couldry & Hepp, 2017), the media practice approach provides a general analytical framework to understand the creation of meaning within societies in and through media. A more detailed definition by Mattoni (2012, p. 159) specifies this view by explaining that media practices are:

> (1) both routinised and creative social practices that; (2) include interactions with media objects (such as mobile phones, laptops, pieces of paper) and media subjects (such as journalists, public relations managers, other activists); (3) draw on how media objects and media subjects are perceived and how the media environment is understood and known.

Media practices are often routinized but can also be used to realize citizen agency. Here, the media practice approach echoes structuration theory (Giddens, 1986), claiming that a key aspect of social order is constant reproduction (routine)

and production (potential change). So far, communication research shows a preference for using the media practice approach to investigate political agency and a change in dominant power structures. Recently, scholars have devised studies on technology activists (Milan & Hintz, 2013; Kubitschko, 2015) and political movements (Mattoni, 2012) and surveillance studies scholars have questioned how people interact with technology by analyzing tactics of resistance to surveillance (Ball, 2005; Martin et al., 2009).

The media practice approach treats media as a structured, yet malleable, context interrelated to social action. Thus, similar to the STS argument, technology can be regarded as 'displaced politics' (Nahuis & van Lente, 2008) and communication and media scholars have poured this emerging relation between politics and individuals into the concept of digital citizenship (Hintz et al., 2019), which denotes the realization of participation and democracy in the digital age. While some approaches to digital citizenship highlight the liberating forces of technology, complex sets of sociopolitical transformations of datafication – incorporating users' personal data into mechanisms of capitalist exchange and governance – pose a tremendous challenge to citizen agency. Hintz et al. (2019, p. 3) pursue the notion that

> [d]atafication 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.

Linking digital citizenship and media practices requires further operationalization. Among the most diverse approaches to grasping media practices stand out by distinguishing media practices according to their political quality (Kubitschko 2017; Kannengießer & Kubitschko 2017;). 'Acting with media' refers to practices of simple use of particular technologies or infrastructures. By contrast, 'acting on media' denotes media practices aimed at shaping media infrastructures, i.e. hacking (Kubitschko, 2017). Acting on media also addresses the discursive level of action that contributes to discourses on media, i.e. on surveillance technologies (Möller & Mollen, 2017). Finally, privacy, as media practice, implies not only technology-oriented action aiming at control over the flow of information but also individual or networked practices of non-use of particular media (we call these 'opting out of media').

Combining approaches to privacy as self-determination with the media as a practice approach, we define 'doing' privacy as technology-oriented human action aiming at control over the flow of personal information. As privacy implies media uses of acting with or acting on media, it is an act of self-determination

and an expression of participation and engagement in public. Beyond that, doing privacy not only depends on others and their communication practices but also impacts on others' privacies, and therefore is always collective.

METHODS

To explore self-determination and privacy as media practice, we conducted a qualitative interview-based study with privacy activists. We understand privacy as a concept referring to the management of informational flows in a critical manner. In other words, 'doing' privacy is to 'make attempts' to realize this via routinized practice and attached meaning. Guided by an in-depth open questionnaire, we sought to answer two research questions (RQs):

- (RQ1): What are citizens' repertoires of doing privacy? In particular: how is privacy achieved by acting with, on, and opting out of—media?

We analyze mundane repertoires of privacy media practice that consist of: (1) using predetermined infrastructures (both hardware and software); (2) setting up own tools or modify existing infrastructures by technological means like encryption; (3) resigning from particular media considered potentially risky in specific situations. The aim is to elicit responses that sketch the broader context of the limits of realizing self-determined privacy in datafied societies.

- (RQ2): Which contextual factors shape privacy practice? How is privacy approached as a relational construct?

This RQ addresses how particular socio-contextual factors play out in how people conduct their privacies. RQ2 reconstructs the ways media practice is given meaning as a private or public affair.

To answer these RQs, we conducted 35 in-depth semi-structured interviews (IDI) with German (n=4) and Polish (n=31) activists working in the fields of privacy, data protection and digital citizenship as members of various NGOs and art and hacker collectives.

Each interview lasted 45–60 minutes and was conducted depending on the preferences of the interviewees either face-to-face or online via end-to-end encrypted communication. There were two tranches of interviews. The first comprising the four Germans and the first five Poles was conducted in 2018. The second comprised the remaining Poles occurred in 2022. The design of the study used inductive coding to analyse the interviews: starting with the distinction of acting with and acting on media practices. After the tranche of interviews, we reconsidered the coding scheme by deepening questions on self-determination

and agency in the context of datafication challenges that people active in online public environments have to overcome.

The activists were not only professionals working for privacy-sensitive non-profit organizations, but also independent activists promoting issues of cybersecurity, encryption and privacy. The study coded the interviewees to protect their anonymity, which enabled IG 1-4 for the German interviewees and IP 1-31 for the Polish ones. The study used the snowballing method to recruit remaining interviewees (n=22). The researchers conducted the IDIs in the participants' native languages structured around common contexts—cultural, social, technological—in order to produce rounded yet reliable understandings based on rich, nuanced and detailed data (Patton, 2002). However, despite having interviewees from two countries in the sample, a cross-national comparison was not our intention, as we explain below.

The study offers a purposeful sample (Patton, 2002, p. 45) that is based on three conditions. The interviewees: (1) reflect on their privacies on an everyday basis; (2) have a considerable level of technical expertise to let them reconstruct a broad repertoire of privacy-related media practices; (3) experience everyday tension regarding how to stay secure and remain visible to the public. Our sample fits Bennett's (2008) taxonomy of privacy advocates' roles: activists, technologists, consultants, researchers, journalists and artists, with a focus on the initial three (see Appendix).

By employing the IDIs, we sought to understand the privacy practices of people that are both highly skilled and aware of technological, political, and cultural aspects of privacy and its violations. The interviewees' views and practices arguably differ from those realized by larger populations on an everyday basis. Their expertise, however, is crucial to recognize not only how the most reflexively skilled understand, evaluate, and do privacy, but also provides nuanced insights into the contradictory nature of the phenomenon. The study seeks to reconstruct a holistic view of privacy, reaching beyond dialectical simplifications of "a them-and-us binary', where 'they' watch 'us', intrude on our privacy" (Lyon 2018, p. 173). The study also aims to reconstruct people's practices with detailed knowledge about their own environments, which will help to explain results previously seen as paradoxical (Kennedy et al., 2017).

FINDINGS

The subsequent analysis explains the interviewees privacy practices (in the following simple 'practices') along the dimensions of 'reflexivity', 'acting with and opting out of media' as well as 'acting on media'. Any of these practices illustrates the relational, contextual and compository character of privacy. Beyond

that, each of them hints at the dilemma of balancing data security and public participation. While the activists' most important motivation is to make sure they can control the flow of their individual or organizational information, they still wish to remain publicly seen and heard and to participate in social and political life. Against this background, privacy is regarded as a constantly evolving endeavor rather than a permanent solution or state.

REFLECTION AND ANALYSIS

Privacy is inseparably related to the reflexive analysis of communication infrastructures and individual routines. Reflection and analysis refer to four dimensions. First, the interviewees carefully and constantly consider threats, risks and benefits emerging from surveillant assemblages built into digital infrastructures. Reflection and analysis are not limited to challenges of individual data security, but always integrate the larger societal picture. Commercial and governmental agents leverage technologies to harvest and analyze sizeable amounts of user data. From the interviewees' viewpoint, both have political implications.

Overall, Polish activists tend to emphasize corporate surveillance with "no handbrake built in it" (IP2) while perceiving state institutions as incapable of mastering technological challenges (IP1, IP2, IP3, IP6, IP17, IP30, IP31). This alleged incompetence may lead to additional potential threats. One interviewee "would feel much better if people that invigilate [them] were competent (…) [because] state-harvested data leak eventually" (IP3), another (IP31) describes state institutions in terms of privacy protection as "stable as a paper house". German activists see threats through both commercial and state surveillance while repeatedly linking it to the historical experience of massive state surveillance in Eastern Germany (IG1, IG2, IG3), a sentiment, interestingly, shared by some Polish activists (IP3, IP5, IP16), referring to personal data storage during communist times. We find these attitudes interesting and coherent, yet also more as a starting point for more comprehensive research on how shared surveillance and privacy imaginaries are tied to historic surveillance experience of users.

Privacy activists have the conviction that the public do not have access to the detailed information on how this surveillance assemblage operates. Consequently, the activists strive to understand and extrapolate these implications. Most of the interviewees emphasise the rapid development of the assemblages during the COVID period and that post-pandemic the privacy-invasive solutions that replaced social contact were not dropped. In this context, not only is technology problematic, but also the political precedent of passing privacy-sensitive biometrical data of citizens to private companies like airlines, which "may lead to other acts of sorting people by the criterion of their health" (IP21), exposing in the broader context "conflicting values of privacy and public health" (IP19).

Beyond structural analysis, interviewees parse their own media and communication repertoires and consider whether they appropriately balance data security and participation options. Considering specific technological, political, and cultural conditions, the shared aim is to reach the highest possible level of data security without societal isolation.

The insight that there is no fixed privacy solution or general rule of use or non-use is key. A German interviewee, for instance, stated that an organization's refusal to respond to e-mails sent from a journalist's Gmail account, as '*simply ridiculous*' (IG2). By contrast, many interviewees' organizations use Gmail's infrastructure because it's stable and secure and, as an interviewee, IP1 explains "The NSA [US' National Security Agency] is not at the top of our potential threats list". Consequently, the need for analysis increases when crossing national borders. "[S]ome countries oblige me to reveal my passwords password [… I need to take care that the hardware I travel with is free of private data". The interviewees possess various sets of hardware for differing contexts. Many use separate computers for international travelling, because crossing national borders means entering new jurisdictions that require empty or better secured equipment. This complex relationship between physical space and privacy also influences decisions about whether to use (or avoid) specific software on mobile devices that easily collect geolocation data (IP26, IP30).

Everyday reflection on how to remain secure comprises constant decision-making on complex people-technology dialectics affecting individual privacy practices. Yet, "safety-wise, tools are comfortable or they are safe" said IP5. Though demanding considerable time and skills, building alternative media practices and privacy routines do not seem to put a strain on everyday communication: "If you are used to it, that is just daily business" said IG1. However, most interviewees recall decisions on compromising privacy because of the convenience of using less safe solutions: "I stopped encrypting e-mails, too lazy for that now" said IP19. A lack of resources, including money, is critical: "I can't afford professional graphics software and I use free one, so I pay for it with my personal data" explained IP8, or time safe solutions "[that] piss me off, because for me time is crucial" stated IP29). The latter tension may be dramatically serious, as IP16, an environmental activist, raged: "the world is coming down and if you want it to persevere a bit longer, you put all your energy into activism and there's not much space left [for learning new, safer solutions]".

Yet, the willingness to reflect and analyze surroundings and routines increases with experienced privacy interventions. When children become part of the game, for instance, "you become more vulnerable" said IG2, while public and private pressure to share data with doctors, daycare or family photo-sharing groups increases.

This leads us to reflection on the inherently relational nature of datafied privacy. If surveillance tools are embedded into online technologies, then managing the limits of own data flows also depends on the practices of other people. Simple actions like taking selfies, sending files, etc. become relevant, as they may weaken or destroy others' privacy. One aspect of this collective nature of privacy is revealed by technological choices: the "golden ideal is using 100% tools with the end-to-end encryption", explained IP1. Yet, there are unsecure communication situations that "can't change, because not everyone uses encryption" argued IG2. Another aspect, and one perceived by most interviewees as of increasing importance, concerns privacy violations by practices of other users. These may occur in professional contexts as after in the aftermath of the pandemic, distant working solutions like desk-time tracking apps or online meetings software may have led to power abuse by office managers or colleagues. However, privacy violations also occur in private (family, friends, etc.) networks, in which the new norm of sharing personal information (Lyon, 2018) is potentially harmful to everyone involved in such exchanges of photos or other personal content. The interviewees also felt other people violated their privacy by persistent demands to respond to their messages: "(…) today, we take away from each other the right to be unreachable" explained IP22. In other words, "it's a matter of awareness. […] [people] violate not only their privacy but also those of others. Like when taking photos at parties and posting them online […]. It's all about our decisions, of all of us" said IP1.

Privacy activists dispose of comprehensive resources to reflect over and analyze privacy risks. One challenge is that this is a constant endeavor, a never-ending story. While activists predominantly communicate within their privacy-aware networks, they save on those resources. Investing time and energy in the public engagement, they cannot rely on "secure" behavior in their networks. Thus doing privacy means constant reflection on how to balance "acting with" potentially unsecure media.

ACTING WITH AND OPTING OUT OF MEDIA

Acting with media denotes practices of managing the flow of information by use of existing, predefined media – both hardware and software. In privacy, acting with and opting out of media, i.e., decisions on not to use or omit particular media, are closely intertwined.

Balancing acting with and opting out practices means repeated decision-making between "being seen" and "being secure". This participatory privacy dilemma points to privacy as a norm on the one hand, while operating in datafied publics threatens individual data security on the other. This challenge is important to

both individuals and organizations that "play visibility games" to use Cotter's (2019) term, practices aiming at gaining attention while risking privacies.

Our interviewees unanimously criticized global digital companies for data harvesting business models, manipulating users' behavior, narrowing public discussion, supporting narcissism and voyeurism. Beyond that, they perceived platform users' everyday practices as a structural support for the social, economic, and cultural position of digital companies. Consequently, some interviewees had never had or deleted their private social media accounts in order to avoid present or future surveillance. They also had the option of paying digital companies with their data and either or both choose free and encrypted tools instead.

Despite their critical attitudes, many interviewees felt forced to use platforms not only by the normalization of being visible online or mutual sharing (Lyon, 2018) but also by direct suggestions made by other agents. For example, the publishing house that employed IG4 was not supportive in helping to realize the expectation to develop a professional Facebook profile. Many other of the interviewees recalled such negative sentiments and admitted they felt pressure from their bosses or professional colleagues expecting them publishing more private information (e.g., photos, and from private contexts like vacations) to gain more outreach in social media. A few interviewees intentionally published carefully chosen private information (like photos depicting their children or private spaces of their homes) to sustain relations with their audience. One interviewee confessed to revealing herself in a private context because "online communication has a native nature" (IP22) and this tactic reflects findings on the growing role of authenticity (the impression of 'realness') as the key resource for people seeking to engage with others (Marwick, 2013). These practices reflect that social media platforms have become the key tool for reaching targeted audiences and promoting projects. The interviewees used social media this way while admitting it also harmed their privacies as most digital platforms have been designed for personal information sharing. Performing professional (or civic) activities on those platforms makes private accounts overexposed to others: "Social media shatter my work-life balance" complained IP27. Post-pandemic platformization of educational activities leads to recording enormous volumes of video materials later published online and, as some interviewees noted agents offering marketing solutions for economic and political agents have already used that footage as bio- and psychometric data.

Yet, the interviewees knew the tools platforms offered came with a price that may affect an organization's integrity. To protect its supporters' privacy, for example, Panoptykon Foundation, does not embed YouTube videos in its website as it would enable extracting cookies of users just entering the site by Google, YouTube's parent company. Instead, the Panoptykon Foundation publishes audiovisual screenshots, links and the transcripts of complete materials. Nevertheless,

the Foundation's status in this context is ambiguous, as its primary field of operation is privacy protection and opposing excessive surveillance:

> Our position is complex. As a foundation, we do use social media […] and are aware that we pay – this way or another – for their services so that our content is visible. And yes, we are aware that these services are possible only because the company performs surveillance activities on its users. (IP4)

Another reason to opt out of media can be an application's sheer size. Even relatively secure technology may be regarded as dangerous when it becomes popular. An insightful case is reported by a German interviewee:

> The CCC [Chaos Computer Club] operates a Jabber server that was used for secure communication by Snowden and Manning. When this turned public hundreds of people started creating accounts. Finally, the CCC decided to close registration, as a bigger size would have meant following other (German) jurisdictions on operating services, such as implementing tools that can be used for surveillance. (IG2)

This tension is unavoidable. Progressing datafication makes acting with and opting out of media imply constantly balancing both with a view to being open to the risks of potential isolation from political communication. As IG2 suggested "I don't want to be [seen wearing] a tin-foil hat". In a similar vein, IP2 stated, "you eventually face the wall –using a mobile phone, you (…) are not going to carry a Faraday cage, are you". Yet, many interviewees who referred to 'sacrificing' their data security by using platform media, still emphasized the specific type of agency they gain through opting out practices. The potential media refusal in mind, they gain a feeling of control over the flow of their individual data. The interviewees mentioned a sense of freedom, despite or even through i.e. the avoidance of taking selfies with others at parties, and not talking to journalists in private surroundings. "This dilemma, in summary, is positive because it's a privilege to talk to the public and still a privilege to protect certain communication very strictly" (IG2). Feelings of self-determination, thus, do not result from definitive security, but from a constant reflection on acting with and opting out of media.

ACTING ON MEDIA

Finally, privacy-oriented media practices comprise various kinds of acting on media, that is, modifying pre-existing services and technologies or creating new ones. Most interviewees secure their communications with encryption of various degrees to achieve a "reasonable compromise" (IP2) between data safety and situational demands. The interviewees reconfigured software and hardware they used in particular contexts, and some of them implemented social mechanisms of improving safety, like organizing key-signing parties for social legitimization of Pretty Good Privacy (PGP) encryption users. Organizations represented by the interviewees create or adjust tools for their own purposes and provide remote configurations of routers for people (journalists, whistleblowers) with whom they communicate. These media interventions are political acts of their own, as they question predetermined ways of how particular technologies work. They are not only attempts to control own and others' private information, but also adjustments of how society deploys technology as a resource.

Our interviewees, however, emphasised how difficult it is to redesign established privacy ecosystems. First, corporate services are usually closed for external modification. Second, it is difficult for free alternatives to reach the needed critical mass of users. The interviewees perceive privacy ecosystems as relatively fixed and immune to direct change. This puts forward the awareness raising, education and discursive activities – the pursuit of privacy, more than technological, is perceived as an endeavor that is "cultural" (IP3), "inherently citizen" (IP26) as well as "discursive and democratic" (IP1).

Technology creates a context for human action that is malleable. The interviewed activists question privacy ecosystems by various acts on media – more often, however, on levels of reflexivity and education than on the level of direct technological adjustment. The issue is more concerned about decisions regarding, which predefined technological solutions to use and which to omit – always in particular contexts – than how to modify them. As the system is less malleable and less open than desired, the structural change in the long run becomes more routinized, mundane and integrated into daily customs and procedures, media practices.

CONCLUSIONS

This study reconstructs the everyday privacy management of privacy-aware agents and, against this background, reveals the potentials and limits of self-determined privacy in datafied societies. Our findings represent insights of agents that approach privacy as a contemporary key theme, and who realize their privacies are a part of professional and social networks with critical views towards

contemporary practices of data collection and analysis. Activists' practices, thus, arguably differ from those realized by larger populations in many regards. The interviewees repeatedly referred to the distinction between the more privacy-aware people and the 'others'. The insights derived from this case can still be used to reconstruct how skilled and aware citizens approach privacy, and in a broader context, to provide knowledge on tensions that datafied citizen agencies realize.

Conceptualizing privacy as media practices contributes to emerging directions in communication and media research. Pioneering studies in this field (Marwick & boyd, 2014) have shown that when trying to understand privacy related decision-making it is worth considering it in the context of everyday relations and affordances. In contrast to approaches that relate privacy practice to specific contexts, this approach shifts the focus to the complex and seemingly contradictory decisions people take to realize privacies. Thus, for instance, using four types of practices (reflecting on, acting with, opting out of and acting on media) may shed light on privacy as critical media practice. Using this background, the study also underlines that privacies of aware and skilled social agents, just like those that regular users realize, are notoriously incomplete. Privacy is not a state, but 'done' in dynamic contexts, and, thus calls for constant adaption. This concerns dynamic technological environments but our study also confirms earlier research on privacy attitude and practical differences (Trepte et al., 2017) across cultures.

Coping with the everyday endeavor that privacy represents, the interviewees explain the role reflection and analysis play for self-determining data and communication flows. Our study reveals various evaluations on whether privacy related care work is a particular burden. Some interviewees admitted, they do not secure their data sufficiently due to a lack of resources, including money, and time, or to a lesser extent, skills. To others, however, privacy work does not feel like a burden, and they acknowledge the investment of time and energy. It is rather a political or democratic attitude towards technology they put forward, a stance that subordinates technology to human needs. The remarkable aspect beyond that is that self-determination can but must not be based in conscious and skillful reflection and decision-making, as Masur 2020 suggests. Self-determination may be carried by networks of alternative media practices, in which reflection over privacy values and means is an inherent part of communication and offers secure spaces for the interviewees (e.g. families, see Kumar et al. 2020). Nevertheless, these networks do face limits. The communities of some of our interviewees grew too big and thus became insecure or the communication with the broader public was interrupted. In line with the earlier studies, the interviewees considered losses of control over their data. Data security is but one dimension of privacy, as building walls would equally mean social isolation or loss of public visibility.

Self-determined privacy, therefore depends on, and is limited by, others. This clearly leaves ideas such as the privacy paradox behind, as the paradoxical is not added to privacy but is inherent in social relations that determine privacy. Having a considerable level of technical expertise is not a precondition for self-determined privacy, but rather facilitates accessing privacy supportive networks.

Our study revealed the tension concerning a new norm and accompanied practices of visibility in datafied environments: staying visible online – and, thus accessible to a broader public when acting the role of a citizen – means constant everyday decisions on compromising privacy and gaining or sustaining social outreach. This tension becomes a complex and challenging aspect of datafied agency that emphasizes two aspects of privacy. First, the collective nature of privacy (an increasing number of others' practices can violate a person's privacy). Secondly, the socio-technological changes that have emerged after the pandemic, such as the introduction of distant working and learning solutions have further challenged people's privacies and tied them to how relations of power are executed.

As Kennedy et al. (2015) argue, "given the ubiquity of social media and its underpinning mechanism of datafication, we need to be attentive to the diverse engagements with data, especially within key fields of public space" (p. 2). In this broader context our research exposes complex, techno-cultural arrangements between people and their personal data flows. In this context, focusing on privacy practices as acts of self-determination helps switch from talking about losing privacy to managing (citizen) publicity, where scholars may consider doing privacy are carefully crafted practices of self-presentation (Marwick, 2013). It also helps keep a critical perspective of how these – reflexive and always contextual – practices are bound to material conditions of being online. Altogether, in the broader perspective, this study sheds light on privacy as an inherent element of datafied citizenship, the key dimension of future communication and media privacy research.

There are limitations to our study – the sample members are arguably more skilled and aware than any larger population and thus, the study cannot make any generalized claims. Also, while interviewing citizens from two different countries, we do not highlight national differences on practices performed unless we can make credible arguments on how they affect a context of reconstructed practices. This strategy also let the study disregard any imbalance in terms of nationality in the sample. Similarly, we did not highlight the types of organizations, for which our interviewees worked, unless it helped to understand a particular communicative practice in question and thus served as 'telling' example supporting more general argument in line with the realist approach to qualitative research (Emmel, 2013). However, we still believe the outcomes are insightful, as reconstructing what people do with media helps to realize 'the opportunities and limitations of actors' practices related to media

technologies and infrastructures for political engagement in a media-saturated society' (Kubitschko 2017, p. 5).

ACKNOWLEDGES

This research is supported by the Polish National Science Centre, Poland (Narodowe Centrum Nauki) grant no. 2020/37/B/HS6/00941 as well as by the TU Dresden University of Technology Disruption and Societal Change Center (TUDiSC).

REFERENCES

Ball, K. (2005). Organization, Surveillance and the Body: Towards a Politics of Resistance. *Organization*, *12*(1), 89–108. https://doi.org/10.1177/1350508405048578

Balleys, C., & Coll, S. (2017). Being publicly intimate: Teenagers managing online privacy. *Media, Culture & Society*, *39*(6), 885–901. https://doi.org/10.1177/0163443716679033

Banks, J. (2015). The Heartbleed bug: Insecurity repackaged, rebranded and resold. *Crime, Media, Culture*, *11*(3), 259–279. https://doi.org/10.1177/1741659015592792

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, (11)9. http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312

Bennett, C., (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Cotter, K. (2019). Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram. *New Media & Society*, *21*(4), 895–913. https://doi.org/10.1177/1461444818815684

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

Couldry N., Hepp A. 2017. *The mediated construction of reality.* Cambridge, Malden, MA: Polity.

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

Dourish, P., Grinter, R. E., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391–401. https://doi.org/10.1007/s00779-004-0308-5

Emmel, N. (2013). *Sampling and Choosing Cases in Qualitative Research. A Realist Approach*. London: SAGE.

Gallagher, K., Patil, S., & Memon, N. (2017). *New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network*. 15.

Giddens, A. (1986). *The Constitution of Society. Outline of the Theory of Structuration*. University of California Press: Berkeley.

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

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*, *35*(1), 3. https://doi.org/10.1007/s13347-022-00497-4

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

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. doi.org/10.17645/mac.v5i3.1165

Kennedy, H., Poell, T., & van Dijck, J. (2015). Data and agency. *Big Data & Society*, *2*(2). https://doi.org/10.1177/2053951715621569

Kennedy H., Elgesem D., Miguel C. 2017. On fairness: User perspectives on social media data mining. *Convergence*, *23*(3), 270–288. https://doi.org/10.1177/1354856515592507

Kubitschko, S. (2015). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence, 21*(3), 388–402. https://doi.org/10.1177/135485651557984

Kumar, P. C., Subramaniam, M., Vitak, J., Clegg, T. L., & Chetty, M. (2020). Strengthening Children's Privacy Literacy through Contextual Integrity. *Media and Communication*, *8*(4), 175–184. https://doi.org/10.17645/mac.v8i4.3236

Lyon, D. (2018). T*he Culture of Surveillance. Watching as a Way of Life*. Cambridge: Polity

Marwick A. (2013). *Status Update*. New Haven, CT: Yale University Press

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

Martin, A.K., van Brakel, R.E., Bernhard, D. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society, 6*(3). https://doi.org/10.24908/ss.v6i3.3282

Masur, P. K. (2020). How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

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

Milan, S., Hintz, A. (2013). Networked Collective Action and the Institutionalized Policy Debate. Bringing Cyberactivism to the Policy Arena? *Policy and Internet*, *5*(1), 7–26. doi.org/10.1002/poi3.20

Möller, Johanna E. (2024 a). Privacy. In Alessandro Nai; Max Groemping; Dominique Wirz (Eds.) *Encyclopedia of Political Communication*, SAGE (forthcoming).

Möller, Johanna E. (2024b). Situational privacy: theorizing privacy as communication and media practice. *Communication Theory*, 34(3), 130–142. https://doi.org/10.1093/ct/qtae011

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.

Nahuis R, van Lente H. (2008). Where Are the Politics? Perspectives on Democracy and Technology. Sci*ence, Technology, & Human Values*, *33*(5), 559–581. https://doi.org/10.1177/0162243907306700

Nippert-Eng C. 2010. *Islands of Privacy*. The University of Chicago Press: Chicago.

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Patton M. 2002. *Qualitative research & evaluation methods*. Sage.

Pink, S., Hjorth, L., Horst, H., Nettheim, J., & Bell, G. (2018). Digital work and play: Mobile technologies and new ways of feeling at home. *European Journal of Cultural Studies*, *21*(1), 26–38. https://doi.org/10.1177/1367549417705602

Sevignani, S. (2015). *Privacy and Capitalism in the Age of Social Media* (Illustrated Edition). Taylor & Francis Ltd.

Tiemann, A., Melzer, A., & Steffgen, G. (2021). Nationwide implementation of media literacy training sessions on internet safety. *Communications*, *46*(3), 394–418. https://doi.org/10.1515/commun-2021-0049

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). https://doi.org/10.1177/2056305116688035

Trepte, S. (2021). The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances. *Communication Theory*, *31*(4), 549–570. https://doi.org/10.1093/ct/qtz035

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

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, *28*(1), 10–29. https://doi.org/10.1177/1095796018819461

APPENDIX

Overview of the interviewees

alias	role	country	when conducted
IG1	activist	Germany	2018
IG2	activist, technologist	Germany	2018
IG3	activist, technologist	Germany	2018
IG4	activist, consultant	Germany	2018
IP1	technologist, consultant	Poland	2018
IP2	technologist	Poland	2018
IP3	activist, technologist, artist	Poland	2018
IP4	activist, consultant	Poland	2018
IP5	technologist	Poland	2018
IP6	activist, consultant	Poland	2022
IP7	researcher, consultant	Poland	2022
IP8	activist, consultant	Poland	2022
IP9	researcher, consultant	Poland	2022
IP10	technologist, consultant	Poland	2022
IP11	activist	Poland	2022
IP12	activist	Poland	2022
IP13	researcher	Poland	2022
IP14	researcher	Poland	2022
IP15	researcher, consultant	Poland	2022
IP16	activist	Poland	2022
IP17	activist, consultant	Poland	2022
IP18	lawyer, consultant	Poland	2022
IP19	lawyer, activist	Poland	2022
IP20	journalist	Poland	2022
IP21	researcher, activist	Poland	2022
IP22	consultant	Poland	2022
IP23	activist	Poland	2022
IP24	researcher, consultant	Poland	2022
IP25	lawyer, activist	Poland	2022
IP26	activist	Poland	2022
IP27	researcher, consultant	Poland	2022
IP28	activist	Poland	2022
IP29	consultant	Poland	2022
IP30	consultant	Poland	2022
IP31	lawyer, activist	Poland	2022