

Inequalities in privacy cynicism: An intersectional analysis of agency constraints

Big Data & Society
January–March: 1–13
© The Author(s) 2024
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20539517241232629
journals.sagepub.com/home/bds



Christian Pieter Hoffmann¹, Christoph Lutz² 
and Giulia Ranzini³

Abstract

A growing body of research highlights a trend toward widespread attitudes of privacy cynicism, apathy and resignation among Internet users. In this work, we extend these discussions by concentrating on the concept of user agency. Specifically, we examine how five types of structural constraints—interpersonal, cultural, technological, economic and political—restrict user agency and contribute to the prevalence of privacy cynicism as a common response. Drawing on critical data studies and adopting an intersectional lens, we demonstrate how these constraints disproportionately impact various social groups unequally, leading to a disparate distribution of agency and privacy cynicism. Furthermore, we contend that the sense of powerlessness engendered by excessive constraints on user agency can, in turn, exacerbate user vulnerability to such constraints, potentially initiating a vicious cycle of disempowerment. The article enriches the field of privacy research by linking the traditionally individual-focused and psychological dimensions of privacy with critical surveillance studies and by proposing potential interventions to mitigate privacy cynicism.

Keywords

Privacy, privacy cynicism, intersectionality, agency, surveillance

This article is a part of special theme on Digital Resignation and Privacy Cynicism. To see a full list of all articles in this special theme, please click here: <https://journals.sagepub.com/page/bds/collections/digitalresignationandprivacycynicism>

Introduction

A key premise in online privacy scholarship is that, before sharing information online, users evaluate the perceived benefits and risks associated with the interaction or transaction (Dinev and Hart, 2006). This so-called privacy calculus assumes individual user agency. Acquisti and colleagues (2016: 445) point out that privacy “is not the opposite of sharing—rather, it is the control over sharing.” Moore and Obhi (2012: 546) define agency as “the experience of controlling action to influence events in the environment.” In the privacy calculus, individuals are assumed to have a choice in online transactions (Rust et al., 2002).

However, recent societal and technological developments have markedly increased the intricacy, complexity and opacity of constraints on user agency. For instance, the widespread use of wearable devices (Li et al., 2016; Rauschnabel et al., 2018) and smart technologies has rendered data sharing ubiquitous (Lutz and Newlands, 2021). Data-intensive services like search engines and social media are crucial infrastructures in modern society and

are challenging to avoid (Ozgun, 2019; Van Dijck et al., 2018). The COVID-19 pandemic has also accelerated the digitalization of social contexts such as education and work, fostering the growth of the “platform economy” where data is frequently used for algorithmic control and surveillance (Cameron et al., 2023; Kellogg et al., 2020; Newlands, 2021; Newlands et al., 2020). In such circumstances, data sharing is increasingly inevitable rather than optional.

¹Institute of Communication and Media Studies, University of Leipzig, Leipzig, Germany

²Nordic Centre for Internet and Society, Department of Communication and Culture, BI Norwegian Business School, Oslo, Norway

³Faculty of Social Sciences, Communication Science, Network Institute, Vrije Universiteit Amsterdam, Amsterdam, Netherlands

Corresponding author:

Christoph Lutz, Nordic Centre for Internet and Society, Department of Communication and Culture, BI Norwegian Business School, Oslo, Norway.

Email: christoph.lutz@bi.no



As users experience these constraints on their agency, feelings of privacy apathy, resignation or cynicism abound (Draper and Turow, 2019; Hargittai and Marwick, 2016; Lutz et al., 2020; Ranzini et al., 2023). When individuals feel powerless, resigned and apathetic about privacy, their willingness and ability to engage in privacy protection behavior suffer. For example, as users engage less in critical considerations of privacy implications, they become more likely to accept terms of service despite feeling uncomfortable or insecure about them (Obar and Oeldorf-Hirsch, 2020). Such behavior renders users more susceptible to online risks and exploitation. The disempowerment of users in today's platform society (Van Dijck et al., 2018) can result in a negative feedback loop, as constraints on user agency trigger feelings of cynicism and resignation that leave users more vulnerable to digital surveillance, ultimately further constraining their agency.

However, not all people are equally affected by agency constraints. Some are in privileged positions, allowing them to shrug off constraints, or at least avoid some of their most severe limitations on agency. A few might even benefit from the effects of agency constraints on peers or strangers. Others bear the full brunt of multiple interlocking structural constraints on user agency. Accordingly, privacy cynicism will affect some users more severely than others. Sannon and Forte (2022) show that, while increasing research attention is dedicated to the privacy experiences of marginalized individuals and groups, most studies focus on single identity categories, such as disability or LGBTQ + sexual orientation. Conversely, there is a lack of systematic consideration of privacy across identity categories.

In this article, we draw on intersectionality theory, both more generally (Collins, 1990; Crenshaw, 1989, 1991) and in critical data studies (D'Ignazio and Klein, 2020; Linabary and Corple, 2019; McDonald et al., 2020), as well as surveillance and privacy research (Draper and Turow, 2019; Lutz et al., 2020; Lyon, 2007; Madden et al., 2017; Marwick, 2022; Ranzini et al., 2023) to show how structural constraints on user agency affect social groups in systematically different ways. We heed the call for a multi-level intersectional analysis (Choo & Ferree, 2010; Rodriguez et al., 2016) that takes both structural influences at the macro-level and experiences based on meaningful social categories at the micro-level into consideration. To that end, we will begin by introducing the intersectional perspective, continue by explaining the role of agency in the emergence of privacy cynicism, to then present a model of interlocking structural agency constraints that, we argue, induces an accumulative unequal distribution of privacy cynicism and privacy vulnerabilities.

An intersectional perspective

Intersectionality has become an influential concept in the social sciences. Originating in Black feminist thought

around 30 years ago, especially through the seminal contributions of Crenshaw (1989, 1991) and Collins (1990), the intersectional paradigm has been taken up across many established disciplines such as sociology (Choo and Ferree, 2010; Walby et al., 2012), political science (Dhamoon, 2011; Hancock, 2007), communication research (Ramasubramanian and Banjo, 2020; West, 2023), human-computer interaction (McDonald et al., 2020; McDonald and Forte, 2020) and management and organization studies (Holvino, 2010; McBride et al., 2015). It is also an influential perspective in interdisciplinary research on technology and data, such as science and technology studies (Gaughan et al., 2018), surveillance studies (Crooks, 2022) and critical data studies (Taylor, 2017).

Despite epistemological and methodological divergences (Rodriguez et al., 2016), the core idea of intersectionality is that social categories, such as gender, race and class, do not stand in isolation and do not shape people's identities independently but intersect in complex ways. For example, a Black woman's experiences are not only distinct from those of a White woman but also from those of a Black man (Crenshaw, 1989, 1991). Considering the interplay of gender *and* race, we understand her positionality better, including how gender and racial marginalization can be compounded. Intersectional theory has focused strongly on gender, race and class (Rodriguez et al. 2016), but these are by no means the only social categories whose intersection shapes people's identities and experiences. Additional social categories include age, sexual orientation, religion, disability, nationality, education and personality (Hancock, 2007; Holvino, 2010; Ramasubramanian and Banjo, 2020).

Intersectional analysis takes different forms. It can range from structural and socio-political approaches that critique unequal power relations to micro-sociological or psychological approaches focused on intersecting identity-based experiences, especially among (multiply) "marked"¹ groups such as queer migrants or disabled religious minorities. When it comes to the more structural macro-approach, the notion of "interlocking oppressions" describes how systems of oppression such as racism, sexism and classism work, and thus should be analyzed, together rather than independently (Collins, 1990). This is complemented by micro-level processes of how these structural influences are experienced in situ based on a person's intersectional identity (Dhamoon, 2011). Choo and Ferree (2010) call for a multi-level approach that includes feedback loops and integrates macrostructures with microstructures. Similarly, Rodriguez et al. (2016) encourage research on intersectionality to "move from a solely subjectivity-identity-centred approach to one that encompasses the interplay of subjectivities, micro-level encounters, structures and institutional arrangements" (204).

Heeding these calls and applying them to privacy, a comprehensive intersectional approach investigates (a)

how larger structures, including the technological, economic or political influences outlined below, affect personal experiences of privacy and (b) how a person perceives and enacts privacy in light of their positionality, which is constituted at the intersection of relevant social categories. Despite initial attempts to integrate an intersectional perspective with the study of privacy, such contributions are only in their infancy (Marwick, 2022; McDonald et al., 2020; McDonald and Forte, 2020). Sannon and Forte (2022) argue that privacy apathy or resignation is especially pronounced among marginalized individuals. Examples include economically disadvantaged individuals falling prey to financially tempting Internet scams (Vitak et al., 2018), or undocumented immigrants submitted to government surveillance (Guberek et al., 2018). However, there is a lack of conceptual argument for why the marginalized would be particularly susceptible to feelings of privacy cynicism. In the following, we will attempt to apply an intersectional analysis to privacy cynicism, focusing on agency and agency constraints. This will involve relating the interlocking macrostructures that constrain agency to the micro-level dynamics of disempowerment.

Micro-level dynamics: user agency and privacy cynicism

In recent years, a number of related concepts have been proposed to understand user disempowerment in the context of online privacy. Digital resignation, for example, refers to “the condition produced when people desire to control the information digital entities have about them but feel unable to do so” (Draper and Turow, 2019: 1824). Hargittai and Marwick (2016) describe a rising feeling of “privacy apathy” among young Internet users, who feel that they cannot effectively protect their personal data from online platforms, but use them anyhow, often due to social pressures. Dencik and Cable (2017) propose the concept of “surveillance realism,” for “a simultaneous unease among citizens with data collection alongside the active normalization of surveillance” (763). Here, we will base our discussion on the concept of privacy cynicism. Hoffmann, Lutz and Ranzini (2016) introduced the concept of privacy cynicism based on in-depth focus group data in Germany, defining it as an “attitude of uncertainty, powerlessness, and mistrust toward the handling of personal data by online services, rendering privacy protection behavior subjectively futile” (p. 2). Subsequently, the concept was positioned in the context of institutional privacy concerns (Lutz et al., 2020) and its multidimensionality was empirically consolidated.

Specifically, privacy cynicism consists of four dimensions (Hoffmann et al., 2016; Lutz et al., 2020): (a) *Mistrust*: surveys show that digital platforms, especially social media platforms, are often viewed with little trust or even mistrust (e.g. Ray, 2021). (b) *Powerlessness*:

cynicism arises when one has little or no control over decision-making. In fact, major online companies are widely perceived as remote and powerful entities that can arbitrarily alter their terms of use (Van Dijck, 2013). (c) *Uncertainty*: one’s mistrust toward a more powerful other is aggravated if their behavior is intransparent. In an online context, for example, many users lack the necessary literacy to understand the workings of digital platforms (Steinfeld, 2016). (d) *Resignation*: individuals experiencing a culmination of mistrust, powerlessness and uncertainty may choose to resign, functionally adhering to an interaction’s requirements but psychologically detaching and protecting their sense of self through cynicism (Tyler and Blader, 2000).

This backdrop of privacy cynicism sets the stage for a deeper exploration into user agency, emphasizing how individuals perceive and respond to these challenges. We argue that user agency plays a critical role in the unequal emergence of privacy cynicism. Agency describes a person’s experience of their capacity to purposefully influence the external world (Gallagher, 2000; Moore and Obhi, 2012). Two key elements of agency are especially relevant for its relationship with privacy cynicism: voluntariness and conscious intention. Voluntariness implies the freedom to choose between options (Haggard, 2005). Agency can only be experienced in situations of choice. Voluntariness pertains to the powerlessness dimension of privacy cynicism: Powerlessness implies a lack of choice as users are forced to depend on the decisions of others, such as platforms or government entities (Dencik and Cable, 2017; Lutz et al., 2020). With regard to conscious intention, Haggard (2005: 291) explains: “Effortful cognitive processes of planning and deliberation typically precede their [action] selection.” Conscious intention thus ties to the uncertainty dimension of privacy cynicism: A lack of understanding of the online environment and a concomitant lack of ability to weigh the risks and benefits of the available options (deliberation) implies a lack of agency and induces feelings of cynicism. The concepts of privacy helplessness (Cho, 2021) and privacy fatigue (Choi et al., 2018) directly address this challenge.

To summarize, research on privacy cynicism and related concepts (Hoffmann et al., 2016; Hargittai and Marwick, 2016; Draper and Turow, 2019) points out that users increasingly experience feelings of powerlessness, mistrust and uncertainty when navigating opaque and ubiquitous digital services, in some cases culminating in resignation. We propose that user agency plays a critical role in the emergence of privacy cynicism. A lack of choice and control induces a sense of disempowerment, which is central to understanding the user’s experience. However, users are not equally vulnerable to privacy cynicism and the ensuing vulnerabilities. To understand these disparities, it is helpful to explore *how* user agency is constrained, using an intersectional analysis.

Macro-level structures: agency constraints

We define agency constraints in the context of online privacy as *structural limits to users' ability to autonomously share their data online*. In this section, we differentiate five sources of agency constraints: (a) interpersonal relations, (b) culture, (c) technology, (d) economics and (e) politics (see Figure 1). After introducing each individual source of constraints, we will discuss how they shape users' sense of agency, applying an intersectional perspective. Importantly, as Figure 1 suggests, the five constraints are interlocking (Collins, 1990; Dhamoon, 2011) and thus jointly shape user experiences based on their respective positionality. We will discuss the (accumulative) unequal impact of interlocking constraints on privacy cynicism based on users' intersection of relevant social categories in the next section. Figure 1 visually represents these constraints and their interlocking nature.

Interpersonal constraints

A first constraint is related to what Bazarova and Masur (2020) describe as a “networked ecology”: a growing interdependence of information sharing, where privacy decisions are no longer exclusively vertical but also

increasingly horizontal (see also Marwick and boyd, 2014 on “networked privacy” and Lutz and Hoffmann, 2017 on “passive participation”). In practice, this is exemplified by the widespread success of a digital platform like TikTok, where the practice of “stitching” clips (i.e. reworking existing videos into new content) exposes users to the audiences of strangers, independently from their chosen level of privacy (Marwick, 2022). This type of exposure brings about risks and benefits impossible for the original creator to evaluate (Bazarova and Masur, 2020; De Wolf, 2020).

Beyond public platforms, interpersonal constraints also emerge within intimate circles such as family and friends, where privacy boundaries are often blurred. In such contexts, friendly and romantic bonds may confuse privacy boundaries (Petronio, 2010), especially when one of the parties involved receives relational, reputational or even monetary benefits from sharing content featuring the other (Buchanan et al., 2019). A quintessential example of interpersonal privacy constraints is “sharenting,” the sharing of child-related content on social media by parents and other relatives (Blum-Ross and Livingstone, 2017; Ranzini et al., 2020; Verswijvel et al., 2019). While sharing information about children might lead parents to find information, support and connection (Goggin and Ellis, 2020; Ranzini et al., 2020), it also limits the agency of tomorrow's adults, denying them the option of constructing an autonomous digital identity (Latifi, 2023).

Interpersonal constraints restrict user agency differently depending on a person's positionality. For example, parents whose personal network is composed of individuals with low privacy skills or awareness are more likely to experience severe agency constraints, when it comes to sharing child-related information. This could be the case among younger users or lower-socioeconomic status (SES) individuals due to educational disadvantages. Similar interpersonal constraints can also be experienced if one's community is very active on social media and post more photos and videos of their kids. The pressure to adhere to such group norms might also affect higher-SES individuals. In the case of the sharenting phenomenon, influencers and celebrities may be quite successful at monetizing pictures of their families, which limits the privacy agency of the children involved (Maddox, 2023).

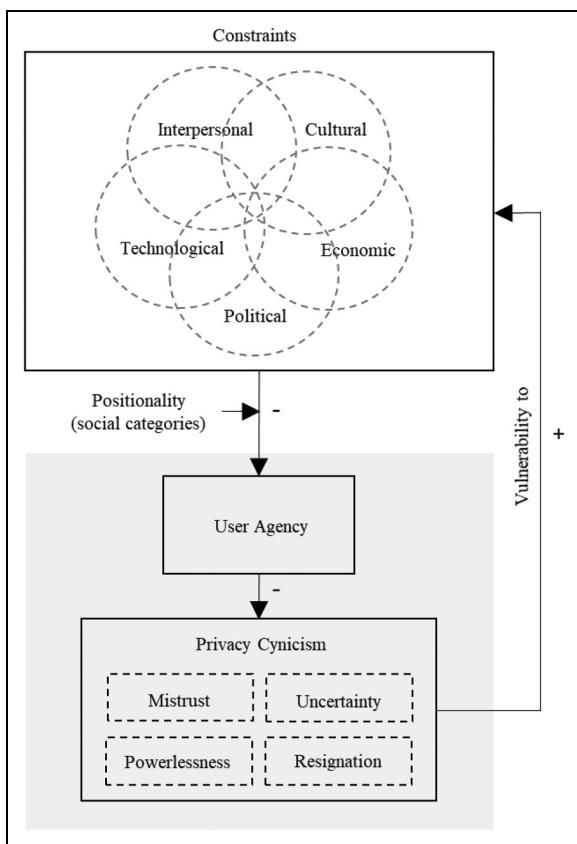


Figure 1. Interlocking constraints on user agency and privacy cynicism.

Cultural constraints

Previous research has emphasized the role of culture in the meaning attributed to privacy. Privacy cultures, identified through patterns in privacy attitudes and behaviors, vary substantially across different regions and communities (Trepte et al., 2017; Vitak et al., 2023). Culture is often operationalized on the country/nation state-level in these studies (Masur et al., 2021; McSweeney, 2002). For example, Miltgen and Peyrat-Guillard (2014) detected a divide between two Southern European (Greece, Spain)

and two Eastern European (Estonia, Poland) countries in terms of perceived privacy control and powerlessness. In Poland and Estonia, respondents reported “a lack of choice, such that they are ‘forced’ to give their data to trusted institutions (e.g. banks, governments, well-known companies)” (115), whereas in Greece and Spain, individuals felt more in control. Even within the same country, culture accounts for a variation in users’ understanding of privacy (Madden et al., 2017), signaling that communities or sociocultural milieus, more than nationalities, might impose values and behaviors when it comes to one’s data online (Lutz, 2016).

Beyond geographic borders, cultural constraints also operate in the domain of digital culture, Internet culture and social media culture, with certain values such as openness, connectivity or emotional engagement either propagated by the user base of communities and platforms (Shifman, 2013), or pushed by the broader technology community (Van Dijck, 2013). Research indicates that much of the digital marketing and platform ecosystem is infused with solutionism and techno-optimism (e.g. Darmody and Zwick, 2020; Zwick et al., 2008). This often results in the under-representation of minoritized groups and creates “privilege hazard,” where certain voices are amplified over others (D’Ignazio and Klein, 2020). The dominant privacy paradigm of digital platforms is one of control and self-responsibilization (Hoffmann et al., 2018; Obar, 2015). The dominance of hegemonic technology narratives in public discourse, often crowding out more critical privacy- and justice-centered voices, constitutes an important aspect of cultural constraints. The recent media hype around OpenAI CEO Sam Altman and the attention Meta’s Yann LeCun receives with his frequently contested social media communication about AI are just two of many examples.

When considering cultural constraints, intersectional dynamics play a key role in shaping privacy cynicism inequality. For example, national cultures can impose norms of openness and transparency that constrain privacy agency. The originally religious Dutch norm of not using window drapes to this day imposes a small, yet noticeable, cultural restriction on immigrants (Van Der Horst and Messing, 2006). Cultural norms are thus entangled with social categories such as gender, race or class. Exploring the intersectional dynamics of cultural constraints, we can see how national cultures and religious beliefs may shape user agency and thus privacy norms. De Leyn (2023) presents a striking example through an in-depth ethnography of young men from ethno-religious minorities in Flanders and their self-presentational and privacy-related practices. Given their societal marginalization, participants try to regain agency through self-presentational strategies such as aligning a hyper-masculine frontstage persona with a more vulnerable backstage persona. These “young men’s selective information

disclosures are informed by negotiations between the ‘self,’ group culture, and racialized discourses across physical and digital spaces” (9).

Another example from the domain of sharenting is the influence of religion, as certain parental practices are shaped by religious norms. For example, Hasanah (2019) defines four principles of sharenting based on Islamic education: “1. Maintain the nature of children (al muhafazoh), 2. Develop children’s potential (al tanmiyah), 3. With clear directions (at taujih), 4. Gradually (al tadaruj)” (47). The first principle speaks specifically to the vulnerable status of children, the second and third to types of content that should and should not be shared (e.g. “Parents should consider not sharing pictures that show their children in any state of undress”: 48) and the fourth to age-appropriate sharing based on specific age ranges of the children (e.g. 0–6, 9–13). In this instance, thus, religiously informed cultural norms may restrict the data-sharing agency of parents, thereby enhancing the privacy of children.

Technological constraints

Technological constraints derive from the architecture of digital technologies and their affordances (Schrock, 2015). Key affordances discussed in privacy literature include visibility, anonymity or persistence/ephemerality. For instance, in terms of visibility, platforms can prioritize certain voices over others through algorithmic curation and content moderation policies (Gorwa et al., 2020). Are (2020) argues that such policies and their enforcement negatively affect vulnerable users, such as sex workers. Drawing on Harvey’s (2019) concept of “aggressive architecture,”² where social media platforms follow a laissez-faire approach rather than protecting their vulnerable users, she discusses how social media platforms doubly disadvantage marked user groups’ in terms of visibility: First, these user groups are exposed to harassment that is not moderated by platforms such as Instagram. Second, their content frequently gets shadowbanned, where “vaguely inappropriate content [...] is hidden from the platform’s explore page” (742), or outright removed. Users who face harassment online also often cannot affect the visibility of harmful content (e.g. Sthapit and Björk, 2019). Online anonymity and pseudonymity are contested (Moore, 2018), especially in authoritarian contexts, but remain popular tools of privacy protection. The affordance of ephemerality (as opposed to persistence), may, on the one hand, allow for more privacy-friendly means of communication, but may also lure users into self-disclosure otherwise avoided (Ma et al., 2021), or be abused for posting privacy-breaching content otherwise not allowed on a platform.

Technological constraints on agency emerge from two primary sources: (a) the ubiquity and pervasiveness of datafication and (b) the increasing autonomy of digital systems: *The ubiquity and pervasiveness* of datafication relates to the

ever-increasing amounts of data generated across different digitized social contexts. Location-based services that run on mobile phones and wearables are increasingly used across domains such as transportation and hospitality (Couture, 2021; Newlands et al., 2019), dating (Ranzini and Lutz, 2017) and commerce (Kim, 2021). The increasing *autonomy* of digital systems is best exemplified by advances in AI and robotics. AI-based technologies are relatively independent and able to engage with humans in sophisticated ways, creating new privacy challenges, for example, in terms of social bonding, anthropomorphism and physical privacy (Lutz et al., 2019). To function properly, many autonomous technologies, such as social robots or autonomous robotic vacuum cleaners, require large amounts of data, both in the development process and during their use. User awareness of these privacy practices can lead to cynical attitudes (Büchi et al., 2022; 2023).

Technological constraints affect user agency not uniformly but are influenced by intersectional dynamics. Social categories such as gender, race and disability significantly influence *design* perceptions, technological *literacy* and levels of *surveillance*, which in turn affect experiences of privacy cynicism. When it comes to *design*, the intersection of visible categories, especially gender and race, is taken up by facial recognition software and existing systems struggle especially with recognizing Black women (Buolamwini and Gebru, 2018). Individuals at the intersection of relevant social categories, such as transgender or disabled individuals, are frequently neglected in technology design, leading to a need for more extensive interactions with platforms or service providers, and thus additional data disclosure. At the same time, technology tailored to the needs of those in need of medical care or individuals with disabilities often come with intimate surveillance, limiting user's privacy agency (Kang and Jung, 2021; Parry et al., 2022).

Technological literacy plays an ever more pronounced role as the technological landscape becomes increasingly complex and opaque. For example, very few users of AI systems (e.g. large language model-based chatbots such as ChatGPT) understand how they function and what their risks are (Burrell, 2016). While users might be familiar, through media coverage or education, with the basic principles of AI systems, their sheer size and complexity as well as corporate secrecy prevent inspection and in-depth privacy literacy (Browne, 2023; Felzmann et al., 2019). Economically disadvantaged individuals might see their purchasing choices limited to products or services with less privacy protection or intransparent data treatment. Educational privileges will, conversely, alleviate some technological constraints due to training and increased literacy. Previous studies also found persistent gender gaps in technological literacy, favoring men (Gnambs, 2021). However, current trends in female educational attainment, with women making significant gains in areas essential

for understanding and engaging with technology, may suggest a potential shift (Siddiq & Scherer, 2019).

Finally, technological surveillance and control are exerted in highly unequal ways (Madden et al., 2017). For example, workers in certain occupations face particularly tight algorithmic surveillance, especially those in the gig economy (Newlands, 2021). Gig economy work is often carried out by migrants and socioeconomically disadvantaged individuals (Newlands, 2022). Technological constraints further erode their privacy, so that relatively high levels of privacy cynicism can be expected in this group. For example, Amazon warehouse workers, who often come from socioeconomically disadvantaged backgrounds, experience meticulous surveillance, measurement and control through pervasive technologies (e.g. augmented reality, robotics). This surveillance is not only a privacy issue but also intersectional one, as it disproportionately affects workers who also belong to marginalized racial or ethnic groups, amplifying their experience of privacy cynicism (Delfanti and Frey, 2021).

Economic constraints

Economic constraints refer to limitations to user agency due to financial incentives that encourage the sharing of personal information, a lack of resource availability or material choice. In the context of “data capitalism”³ (West, 2019), many platforms incentivize the sharing of personal information—it may be a precondition for usage, or it may entail additional benefits, such as personalized services (Rust et al., 2002; Zwick et al., 2008). However, incentives for self-disclosure can be difficult to assess if services do not provide sufficient information, or have intransparent and overly complex terms and conditions (Turow et al., 2023). Crain (2018) argues that platform business models entail structural limitations to transparency as they rely on privacy asymmetry. Increasing awareness of the risks associated with online transactions leads users to want more control (Olivero and Lunt, 2004), which platforms frequently cannot or do not wish to accommodate.

Threats to user agency are especially pronounced when users have limited choice in the use of a platform, for example, due to a lack of alternative services or network effects, where the value of a service increases as more people use it. Under such conditions, users perceive trading privacy for material or immaterial benefits as unfair (Draper and Turow, 2019). Market structures are therefore of critical importance to economic constraints on user agency and privacy (Zuboff, 2019). The platform economy is characterized by high degrees of concentration, winner-takes-all markets and market dominance by few tech giants (Rietveld and Schilling, 2021). Even given a net “positive” privacy calculus, where perceived benefits of self-disclosure outweigh its disadvantages, users may

feel a lack of control due to a lack of choice (Haggard, 2005).

From an intersectional perspective, resource availability constitutes an important boundary condition for the privacy calculus, underscoring the connection between privacy and digital inequality (Lutz, 2019; Park, 2021). Users commanding more resources may find it easier to substitute privacy-threatening online services (e.g. use a limousine service instead of a ride-sharing app), outsource risks to third parties (e.g. hire staff to book services) or obtain additional assurances (e.g. insurance, security software). Social media platforms increasingly position privacy features as a fee-based premium: the Meta Verified subscription service, for example, offers protection against impersonation on Facebook and Instagram (Meta, 2023). Such services indicate the complexity of the economics of privacy (Acquisti et al., 2016). While in some contexts, self-disclosure may offer material benefits, such as access to services or savings, in others, not sharing data may be more rewarding (e.g. avoiding disclosures of price sensitivity).

Users lacking resources, thus, may on the one hand face a need to employ online services to gain access to, for example, job opportunities or more affordable product offers. On the other hand, the price they pay in terms of data might be very high. Madden and colleagues (2017) highlight how low-income American adults rely more on connective services while also abstaining from privacy protection behavior, resulting in a “matrix of vulnerability” (53) that has wider social implications. Studies in the sharing of self-produced sexual content note that differences in income, more than gender, predicted sharing (Blake et al., 2018). The example highlights how material disadvantages intersect with other meaningful social categories, such as gender, race or sexual orientation, to compound privacy vulnerabilities, including privacy cynicism (Moore-Berg and Karpinski, 2019).

Political constraints

Political systems and regulatory frameworks not only define the nature of privacy but also specify the extent to which it is protected and how it can be defended. Of course, the extent and specificities of legal privacy protections differ by jurisdiction (cf. DLA Piper, 2023). Individuals are also subject to multiple overlapping regulatory frameworks (international, national, state and local) that render the specific and situational delineation of privacy opaque and difficult to grasp.

Research on online political engagement in authoritarian contexts highlights how political institutions restrict privacy rights, rather than protecting them. In a case study of Turkey, Kocer and Bozdağ (2020) find that those who support an authoritarian regime are much more likely to engage in political online expression than those who oppose it. Pearce and colleagues (2018) show how political

dissidents in Azerbaijan employ tactics such as maintaining multiple profiles, friends lists or self-censorship to avoid political repercussions. Lokot (2020) highlights how political dissidents in Russia withdraw from digital platforms collaborating with government institutions—triggering political pressures on citizens to maintain digital visibility. From an intersectional perspective, support of or opposition to authoritarian regimes and its privacy implications, is not independent of social categories such as class, gender or ethnicity. In China, for example, gay men worry that the use of location-based dating apps may expose them to persecution (Cummings, 2020). In Iran, women engaging in cyberactivism are particularly vulnerable to political repercussions and thus need to explore ever more innovative approaches to protecting their privacy (Batmanghelichi and Mouri, 2017).

Government infringement on privacy is not a phenomenon unique to authoritarian contexts. Madden and colleagues (2017) highlight how socioeconomically disadvantaged citizens of Western welfare states are regularly subject to privacy restrictions as a precondition for receipt of benefits. This phenomenon is only becoming more prevalent with the digitization of the welfare state (Bagger et al., 2023). Initiatives such as smart cities facilitate public-private partnerships that are based on “extractive data practices” (Artyushina, 2020). In such contexts, data sharing is framed as a public good, where public interests override individual data protection desires (Acquisti et al., 2016). A public interest framing has long been well-established in matters of security, for example, in justifying digital policing practices such as public surveillance, profiling or predictive policing (Brayne, 2017; Browning and Arrigo, 2021). Again, low-SES individuals and ethnic minorities tend to be more exposed to overpolicing.

As Draper and Turow (2019) point out, digital resignation does not entirely preclude protective behavior—they see potential for digital resignation to trigger (at least passive) resistance to surveillance. Today, digital platforms are a critical infrastructure for political engagement (Vaccari and Valeriani, 2021). They can be employed in what Bazarova and Masur (2020, p. 121) term “collective privacy boundary management,” for example, by challenging current political conditions and regulatory frameworks (Beraldo and Milan, 2019). Of course, employing digital platforms to enact collective political agency comes with the conundrum of exposing individuals to many of the agency constraints outlined above, such as peer pressure, mutual tagging and data harvesting (Hoffmann and Lutz, 2023; Neubaum and Lane, 2023). From an intersectional perspective, it is noteworthy that online political participation is socioeconomically stratified (Hoffmann and Lutz, 2021; Oser et al., 2022), so that marginalized individuals or groups are less likely to benefit from “collective privacy boundary management” through online

political engagement. Dencik and colleagues (2016) therefore propose the concept of “data justice” to tie political activism on privacy matters to broader social justice concerns.

Interlocking of constraints, intersection of experiences

Collins (1990) proposed the notion of “interlocking oppressions,” showing how systems of oppression, such as racism or classism, interact in privileging or disadvantaging individuals. Rodriguez et al. (2016) encourage an extension of this perspective to structural and institutional arrangements. We apply this notion to structural constraints on privacy agency. Interpersonal, cultural, technological, economic and political agency constraints should not be analyzed in isolation, but rather in conjunction. For example, an individual living in Iran may be subject to the political constraints of an authoritarian regime, *and* the economic constraints of a developing economy, *and* the interpersonal constraints of the religious stances of friends and family, *and* the technological constraints of impeded access to Western digital platforms. Instead, an individual in China may be subject to the political constraints of censorship and surveillance, *and* the technological constraints of the “Great Firewall,” *and* economic constraints of exploitative work conditions, etc. An individual in the US, finally, may be subject to the technological and economic constraints of ubiquitous online services and platforms under “data capitalism” (West, 2019), *and* political constraints of limited data protection regulation, *and* cultural constraints of techno-optimism and accelerationism. Importantly, interlocking constraints do not simply stack but intersect in complex, often unpredictable ways, creating unique experiences of privacy and agency. This complexity needs to be taken into account to understand someone’s sense of privacy cynicism.

As these examples highlight, and as depicted in Figure 1, there is no uniform way in which interlocking agency constraints impact an individual’s sense of agency and privacy. Rather, structural influences are experienced in situ based on a person’s intersectional identity (Dhamoon, 2011). An intersectional analysis, thus, requires both a macro-level analysis of structural constraints and a micro-level analysis of meaningful social categories to understand systematic inequalities. The experiences of agency constraints and their effect on privacy cynicism in each of the given examples differ based on person’s class, ethnicity, gender or sexual identity, for example. How the listed economic, political, interpersonal, cultural and technological constraints will shape the sense of agency and privacy of an individual in Iran will differ meaningfully between men and women, for example, or a straight or queer person.

The proposed intersectional analysis should not be read as solely contingent on national context. For example, the agency and privacy experience of two individuals in the US will differ systematically not just by meaningful social categories, such as race, gender or class, but also by how these intersectional positionalities change the subjection to structural agency constraints. In other words, a wealthy Black woman in the US will differ in her sense of agency and privacy from a poor Black woman in the US, as they will be exposed to different interlocking cultural, technological, economic and even political agency constraints (e.g. pressure to be online, access to digital platforms, political influence, etc.). Thus, an intersectional analysis of macro-level structural agency constraints and micro-level experiences of agency requires both tolerance for contingency and complexity, and respect for subjective, identity-based positionality (Rodriguez et al., 2016).

Finally, Choo and Ferree (2010) point out that a multi-level approach to an intersectional analysis should account for feedback loops between levels. We, therefore, argue that the effect of interlocking agency constraints on an individual based on their positionality not only induces systematic differences in susceptibility to privacy cynicism, but compounds such inequalities into a negative feedback loop. Heightened levels of cynicism, especially in the form of resignation (Hoffmann et al., 2016; Lutz et al., 2020), will render individuals more vulnerable to agency constraints:

First, cynical users may forgo opportunities to increase their privacy literacy (Masur, 2020), which could help them avoid some of the pitfalls of interpersonal or technological agency constraints. Second, cynical users might ignore their options *despite* agency constraints, such as choices of which platforms to use, how and with which intensity. Each choice, however small, could nevertheless result in marginal improvements in privacy protection. Again, research on surveillance and political activism in authoritarian settings highlights how, even under the harshest conditions, individuals defend some degree of privacy (Kocer and Bozdağ, 2020; Pearce et al., 2018). Third, cynical users are unlikely to challenge structural constraints beyond, possibly, passive resistance (Bazarova and Masur, 2020; Draper and Turow, 2019). Dencik and Cable (2017) show that even political activists are not immune from feelings of resignation. By deterring from political activism and resistance to surveillance, privacy cynicism makes users more vulnerable to structural agency constraints.

Discussion and conclusion

In this article, we applied an intersectional perspective to examine how systematic inequalities in privacy cynicism emerge in today’s platform society (Van Dijck et al., 2018). More specifically, we proposed a multi-level intersectional analysis (Choo & Ferree, 2010; Rodriguez et al.,

2016) that considers both macro-level structural influences and micro-level experiences of agency and privacy based on meaningful social categories (positionality). We explored five interlocking structural constraints on user agency, which are experienced on the micro-level based on a person's positionality, inducing systemic inequalities. A lack of agency is generally related to heightened feelings of privacy cynicism. Finally, we argued that privacy cynicism makes users more vulnerable to agency constraints, creating a negative feedback loop.

To situate our article theoretically, we drew on rich interdisciplinary literature, especially on intersectionality, surveillance and privacy (Collins, 1990; Crenshaw, 1989, 1991; D'Ignazio and Klein, 2020; Linabary and Corple, 2019; Marwick, 2022; McDonald et al., 2020). This adds necessary nuance, showing how agency constraints shape user experiences in variegated ways, depending on structural and identity-based dynamics. Interpersonal constraints, like parents' control over their children's privacy, may manifest in problematic sharenting practices (Latifi, 2023). Cultural constraints, such as media narratives that prioritize progress over privacy, can also erode agency (Dencik and Cable, 2017). Technological constraints capture power imbalances between data collectors and users, affecting user agency through design and literacy (Buolamwini and Gebru, 2018). Economic constraints involve pay-for-privacy schemes that either limit user experience or incentivize over-sharing (Elvy, 2017). Lastly, political constraints arise from power asymmetries between governments and citizens, with intersectional factors like social status or minority status further shaping limitations on data-related choices (Batmanghelichi and Mouri, 2017).

A number of implications can be derived from this intersectional perspective. Addressing constraints on user agency that foster privacy cynicism requires mitigating power imbalances, challenging the existing matrix of domination and empowering those at the margins. The data justice and data feminism literature shows how data science can be used for this goal of co-liberation (D'Ignazio and Klein, 2020; Goldkind et al., 2021). Concretely, such a program includes examining and challenging existing power structures, elevating emotion and embodiment, rethinking binaries and hierarchies and considering context, among others. To put these principles into practice, various stakeholders have a role to play and the best approaches are holistic, combining technical, legal, political and social strategies.

Technological systems include access to privacy-enhancing technologies. Platforms could install warning signs, filters, sophisticated encryption and adopt a philosophy of data sparsity (i.e. prioritize the least data-hungry implementation). Of course, such technological solutions can only alleviate inequality if they are accessible to those especially exposed to agency constraints. Legal solutions

involve stringent data protection laws and enforcement, particularly of vulnerable groups such as children, sexual minorities or disabled people. Legal solutions, however, presuppose political action, which, in turn, requires political agency. Opposition to (authoritarian) surveillance should not be limited to those already in a position of privilege. Social remedies can focus on user empowerment and literacy, especially among marginalized groups. Institutions such as schools, employers and the media can prioritize privacy-related issues, involving civil society and privacy advocacy groups (e.g. by amplifying their voices through featuring them prominently in media coverage or by co-organizing workshops and hackathons in schools or companies). Combining these approaches may combat the inequality emerging from a disempowering feedback loop of structural constraints on user agency and privacy cynicism.

Acknowledgments

We would like to thank the editorial team at *Big Data & Society*, specifically Matthew Zook, as well as Nora Draper and Joe Turow for organizing a very constructive review process. Three anonymous peer reviewers provided useful feedback that greatly strengthened the article.


Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Norges Forskningsråd (grant number 275347, 299178).

ORCID iD

Christoph Lutz  <https://orcid.org/0000-0003-4389-6006>

Notes

1. The concept of "marked" versus "unmarked" is used to distinguish different groups within a social category such as gender or race. Marked is understood as a/the different group that occupies a/the non-hegemonic position and is specifically mentioned and called out as the non-default (McBride et al., 2015), for example, in language or policies. Non-marked, by contrast, describes the hegemonic group that was and still often is conventionally seen as the norm or default. Within the social category of gender, for example, "male" is the non-marked group, whereas "female" and "non-binary" are marked groups. Within the social category of race, "White" is the non-marked group, while "Black" and "Mixed Race" are marked groups.
2. The concept of "aggressive architecture" is adopted from urban planning and design and sometimes called "hostile architecture." Its aim is to discourage "certain kinds of activity in

- public spaces” such as rough sleeping. The Camden bench in London is a quintessential example (Wikipedia, 2023). Applied to digital platforms, Harvey (2019) argues that “active inactivity in dealing with toxic and hateful speech and action in the regulation of these sites is what becomes aggressive architecture as the concerns, needs, and well-being of publics continue to go unaddressed despite their visibility.”
3. West (2019: 20) defines data capitalism as “a system in which the commoditization of our data enables an asymmetric redistribution of power that is weighted toward the actors who have access and the capability to make sense of information. It is enacted through capitalism and justified by the association of networked technologies with the political and social benefits of online community, drawing upon narratives that foreground the social and political benefits of networked technologies.”
- ## References
- Acquisti A, Taylor C and Wagman L (2016) The economics of privacy. *Journal of Economic Literature* 54(2): 442–492.
- Are C (2020) How Instagram’s algorithm is censoring women and vulnerable users but helping online abusers. *Feminist Media Studies* 20(5): 741–744.
- Artyushina A (2020) Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto. *Telematics and Informatics* 55: 101456.
- Bagger C, Einarsson AM, Andelsman Alvarez V, et al. (2023) Digital resignation and the datafied welfare state. *Big Data & Society* 10(2): 1–5.
- Batmanghelichi KS and Mouri L (2017) Cyberfeminism, Iranian style: Online feminism in post-2009 Iran. *Feminist Media Histories* 3(1): 50–80.
- Bazarova NN and Masur PK (2020) Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology* 36: 118–123.
- Beraldo D and Milan S (2019) From data politics to the contentious politics of data. *Big Data & Society* 6(2): 1–11.
- Blake KR, Bastian B, Denson TF, et al. (2018) Income inequality not gender inequality positively covaries with female sexualization on social media. *Proceedings of the National Academy of Sciences* 115(35): 8722–8727.
- Blum-Ross A and Livingstone S (2017) “Sharenting,” parent blogging, and the boundaries of the digital self. *Popular Communication* 15(2): 110–125.
- Brayne S (2017) Big data surveillance: The case of policing. *American Sociological Review* 82(5): 977–1008.
- Browne R (2023) OpenAI CEO admits a bug allowed some ChatGPT users to see others’ conversation titles. *CNBC*, 23 March. Available at: <https://www.cnbc.com/2023/03/23/openai-ceo-says-a-bug-allowed-some-chatgpt-to-see-others-chat-titles.html>.
- Browning M and Arrigo B (2021) Stop and risk: Policing, data, and the digital age of discrimination. *American Journal of Criminal Justice* 46: 298–316.
- Buchanan R, Southgate E and Smith SP (2019) ‘The whole world’s watching really’: Parental and educator perspectives on managing children’s digital lives. *Global Studies of Childhood* 9(2): 167–180.
- Büchi M, Festic N and Latzer M (2022) The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society* 9(1): 1–14.
- Büchi M, Fosch-Villaronga E, Lutz C, et al. (2023) Making sense of algorithmic profiling: User perceptions on Facebook. *Information, Communication & Society* 26(4): 809–825.
- Buolamwini J and Gebru T (2018) Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on Fairness, Accountability and Transparency*: 77–91.
- Burrell J (2016) How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society* 3(1): 1–12.
- Cameron L, Lamers L, Leicht-Deobald U, et al. (2023) Algorithmic management: Its implications for information systems research. *Communications of the Association for Information Systems* 52(1): 23.
- Cho H (2021) Privacy helplessness on social media: Its constituents, antecedents and consequences. *Internet Research* 32(1): 150–171.
- Choi H, Park J and Jung Y (2018) The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81: 42–51.
- Choo HY and Ferree MM (2010) Practicing intersectionality in sociological research: A critical analysis of inclusions, interactions, and institutions in the study of inequalities. *Sociological Theory* 28(2): 129–149.
- Collins PH (1990) *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. London: Routledge.
- Couture J (2021) Reflections from the ‘Strava-sphere’: Kudos, community, and (self-) surveillance on a social network for athletes. *Qualitative Research in Sport, Exercise and Health* 13(1): 184–200.
- Crain M (2018) The limits of transparency: Data brokers and commodification. *New Media & Society* 20(1): 88–104.
- Crenshaw KW (1989) Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum* 14: 538–554.
- Crenshaw KW (1991) Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review* 43: 1241–1299.
- Crooks R (2022) Seeking liberation: Surveillance, datafication, and race. *Surveillance & Society* 20(4): 413–419.
- Cummings J (2020) ‘Now you can see who’s around you’: Negotiating and regulating gay intimacies on mobile media in the People’s Republic of China. In: Cabañes JVA and Uy-Tioco CS (eds) *Mobile Media and Social Intimacies in Asia*. Dordrecht: Springer, 15–30.
- Darmody A and Zwick D (2020) Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. *Big Data & Society* 7(1): 1–12.
- De Leyn T (2023) Reclaiming agency in the digital neighborhood: An ethnographic exploration of ethno-religious minority youths’ performances of the masculine self. *Journal of Computer-Mediated Communication* 28(6): zmad037.
- Delfanti A and Frey B (2021) Humanly extended automation or the future of work seen through Amazon patents. *Science, Technology, & Human Values* 46(3): 655–682.
- Dencik L and Cable J (2017) The advent of surveillance realism: Public opinion and activist responses to the

- Snowden leaks. *International Journal of Communication* 11: 763–781.
- Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society* 3(2): 1–12.
- De Wolf R (2020) Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media & Society* 22(6): 1058–1075.
- Dhamoon RK (2011) Considerations on mainstreaming intersectionality. *Political Research Quarterly* 64(1): 230–243.
- D'Ignazio C and Klein LF (2020) *Data Feminism*. Cambridge, MA: MIT Press.
- Dinev T and Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17(1): 61–80.
- DLA Piper (2023) Data protection laws of the world. Available at : <https://www.dlapiperdataprotection.com/index.html> (04/05/23).
- Draper NA and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.
- Elvy SA (2017) Paying for privacy and the personal data economy. *Columbia Law Review* 117: 1369–1460.
- Felzmann H, Fosch-Villaronga E, Lutz C, et al. (2019) Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society* 6(1): 1–14.
- Gallagher S (2000) Philosophical conceptions of the self: Implications for cognitive science. *Trends in Cognitive Sciences* 4(1): 14–21.
- Gaughan M, Melkers J and Welch E (2018) Differential social network effects on scholarly productivity: An intersectional analysis. *Science, Technology, & Human Values* 43(3): 570–599.
- Gnambs T (2021) The development of gender differences in information and communication technology (ICT) literacy in middle adolescence. *Computers in Human Behavior* 114: 106533.
- Goggin G and Ellis K (2020) Privacy and digital data of children with disabilities: Scenes from social media sharenting. *Media and Communication* 8(4): 218–228.
- Goldkind L, Wolf L and LaMendola W (2021) Data justice: Social work and a more just future. *Journal of Community Practice* 29(3): 237–256.
- Gorwa R, Binns R and Katzenbach C (2020) Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society* 7(1): 1–15.
- Guberek T, McDonald A, Simioni S, et al. (2018) Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–15).
- Haggard P (2005) Conscious intention and motor cognition. *Trends in Cognitive Sciences* 9(6): 290–295.
- Hancock AM (2007) When multiplication doesn't equal quick addition: Examining intersectionality as a research paradigm. *Perspectives on Politics* 5(1): 63–79.
- Hargittai E and Marwick AE (2016) "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication* 10: 3737–3757.
- Harvey A (2019) Tits or GTFO: The aggressive architecture of the internet. *Flowjournal* 24. Available at: <https://www.flowjournal.org/2019/05/tits-or-gtfo-the-aggressive-architecture-of-the-internet-alison-harvey-university-of-leicester/>.
- Hasanah FF (2019) Sharenting in the perspective of Islamic education. *Sunan Kalijaga International Journal on Islamic Educational Research* 3(2): 42–50.
- Hoffmann AL, Proferes N and Zimmer M (2018) "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society* 20(1): 199–218.
- Hoffmann CP and Lutz C (2021) Digital divides in political participation: The mediating role of social media self-efficacy and privacy concerns. *Policy & Internet* 13(1): 6–29.
- Hoffmann CP and Lutz C (2023) The contextual role of privacy concerns in online political participation. *European Journal of Communication* 38(4): 363–379.
- Hoffmann CP, Lutz C and Ranzini G (2016) Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10(4): article 7.
- Holvino E (2010) Intersections: The simultaneity of race, gender and class in organization studies. *Gender, Work & Organization* 17(3): 248–277.
- Kang H and Jung EH (2021) The smart wearables-privacy paradox: A cluster analysis of smartwatch users. *Behaviour & Information Technology* 40(16): 1755–1768.
- Kellogg KC, Valentine MA and Christin A (2020) Algorithms at work: The new contested terrain of control. *Academy of Management Annals* 14(1): 366–410.
- Kim E (2021) In-store shopping with location-based retail apps: Perceived value, consumer response, and the moderating effect of flow. *Information Technology and Management* 22: 83–97.
- Kocer S and Bozdağ Ç (2020) News-sharing repertoires on social media in the context of networked authoritarianism: The case of Turkey. *International Journal of Communication* 14: 5292–5310.
- Latifi F (2023) Influencer parents and the kids who had their childhood made into content. *Teen Vogue*, 10 March. Available at: <https://www.teenvogue.com/story/influencer-parents-children-social-media-impact>.
- Li H, Wu J, Gao Y, et al. (2016) Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics* 88: 8–17.
- Linabary JR and Corple DJ (2019) Privacy for whom? A feminist intervention in online research practice. *Information, Communication & Society* 22(10): 1447–1463.
- Lokot T (2020) Articulating networked citizenship on the Russian internet: A case for competing affordances. *Social Media + Society* 6(4): 1–12.
- Lutz C (2016) A social milieu approach to the online participation divides in Germany. *Social Media + Society* 2(1): 1–14.
- Lutz C (2019) Digital inequalities in the age of artificial intelligence and big data. *Human Behavior and Emerging Technologies* 1(2): 141–148.
- Lutz C and Hoffmann CP (2017) The dark side of online participation: Exploring non-, passive and negative

- participation. *Information, Communication & Society* 20(6): 876–897.
- Lutz C, Hoffmann CP and Ranzini G (2020) Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society* 22(7): 1168–1187.
- Lutz C and Newlands G (2021) Privacy and smart speakers: A multi-dimensional approach. *The Information Society* 37(3): 147–162.
- Lutz C, Schöttler M and Hoffmann CP (2019) The privacy implications of social robots: Scoping review and expert interviews. *Mobile Media & Communication* 7(3): 412–434.
- Lyon D (2007) *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- Ma X, Qin Y, Chen Z, et al. (2021) Perceived ephemerality, privacy calculus, and the privacy settings of an ephemeral social media site. *Computers in Human Behavior* 124: 106928.
- Madden M, Gilman M, Levy K, et al. (2017) Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review* 95: 53–125.
- Maddox J (2023) When sponsored content meets ‘sharenting,’ kids are powerless to stop their influencer parents using them as props. *Fortune*, 18 January. Available at: <https://fortune.com/2023/01/18/influencers-children-social-media-laws-sponsored-content-sharenting/>.
- Marwick AE (2022) Privacy without power: What privacy research can learn from surveillance studies. *Surveillance & Society* 20(4): 397–405.
- Marwick AE and boyd d (2014) Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16(7): 1051–1067.
- Masur PK (2020) How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication* 8(2): 258–269.
- Masur PK, Epstein D, Quinn K, et al. (2021) A comparative privacy research framework. Available at: <https://osf.io/preprints/socarxiv/fjqhs/>.
- McBride A, Hebson G and Holgate J (2015) Intersectionality: Are we taking enough notice in the field of work and employment relations? *Work, Employment and Society* 29(2): 331–341.
- McDonald N, Badillo-Urquiola K, Ames MG, et al. (2020) Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*: 1–8.
- McDonald N and Forte A (2020) The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*: 1–14.
- McSweeney B (2002) Hofstede’s model of national cultural differences and their consequences: A triumph of faith—a failure of analysis. *Human Relations* 55(1): 89–118.
- Meta (2023) Testing Meta Verified to help creators establish their presence. Meta Newsroom, 19 February 2023. Available at: <https://about.fb.com/news/2023/02/testing-meta-verified-to-help-creators/>.
- Miltgen CL and Peyrat-Guillard D (2014) Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems* 23(2): 103–125.
- Moore-Berg SL and Karpinski A (2019) An intersectional approach to understanding how race and social class affect intergroup processes. *Social and Personality Psychology Compass* 13(1): e12426.
- Moore A (2018) Anonymity, pseudonymity, and deliberation: Why not everything should be connected. *Journal of Political Philosophy* 26(2): 169–192.
- Moore JW and Obhi SS (2012) Intentional binding and the sense of agency: A review. *Consciousness and Cognition* 21(1): 546–561.
- Neubauer G and Lane DS (2023) Nevertheless, it persists: Political self-effects in the context of persistent social media. *Journal of Media Psychology* 35(6): 375–386.
- Newlands G (2021) Algorithmic surveillance in the gig economy: The organization of work through Lefebvrian conceived space. *Organization Studies* 42(5): 719–737.
- Newlands G (2022) ‘This isn’t forever for me’: Perceived employability and migrant gig work in Norway and Sweden. *Environment and Planning A: Economy and Space*: 1–18. Epub ahead of print 4 March. DOI: 10.1177/0308518X2210830
- Newlands G, Lutz C and Fieseler C (2019) Trading on the unknown: Scenarios for the future value of data. *The Law & Ethics of Human Rights* 13(1): 97–114.
- Newlands G, Lutz C, Tamò-Larriex A, et al. (2020) Innovation under pressure: Implications for data privacy during the COVID-19 pandemic. *Big Data & Society* 7(2): 1–14.
- Obar JA (2015) Big data and the phantom public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society* 2(2): 1–16.
- Obar JA and Oeldorf-Hirsch A (2020) The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23(1): 128–147.
- Olivero N and Lunt P (2004) Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology* 25(2): 243–262.
- Oser J, Grinson A, Boulianne S, et al. (2022) How political efficacy relates to online and offline political participation: A multilevel meta-analysis. *Political Communication* 39(5): 607–633.
- Ozgun A (2019) [Cntrl]+[Alt]+[Esc]? Virtual platforms as spaces of control and contestation. *Markets, Globalization & Development Review* 3(3): article 1.
- Park YJ (2021) Why privacy matters to digital inequality. In: Hargittai E (eds) *Handbook of Digital Inequality*. Cheltenham: Edward Elgar, 284–294.
- Parry JP, Chen SH, Ku L, et al. (2022) Is telehealth a valuable resource in reproductive endocrinology and infertility? *Fertility and Sterility* 117(4): 690–695.
- Pearce KE, Vitak J and Barta K (2018) Socially mediated visibility: Friendship and dissent in authoritarian Azerbaijan. *International Journal of Communication* 12: 1310–1331.
- Petronio S (2010) Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review* 2(3): 175–196.
- Ramasubramanian S and Banjo OO (2020) Critical media effects framework: Bridging critical cultural communication and media effects through power, intersectionality, context, and agency. *Journal of Communication* 70(3): 379–400.

- Ranzini G and Lutz C (2017) Love at first swipe? Explaining Tinder self-presentation and motives. *Mobile Media & Communication* 5(1): 80–101.
- Ranzini G, Lutz C and Hoffmann CP (2023) Privacy cynicism: Resignation in the face of agency constraints. In: Trepte S and Masur PK (eds) *The Routledge Handbook of Privacy and Social Media*. London: Routledge, 134–143.
- Ranzini G, Newlands G and Lutz C (2020) Sharenting, peer influence, and privacy concerns: A study on the Instagram-sharing behaviors of parents in the United Kingdom. *Social Media + Society* 6(4): 1–13.
- Rauschnabel PA, He J and Ro YK (2018) Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research* 92: 374–384.
- Ray J (2021) Young people rely on social media, but don't trust it. *GALLUP*, 18 November. Available at: <https://news.gallup.com/opinion/gallup/357446/young-people-rely-social-media-don-trust.aspx>.
- Rietveld J and Schilling MA (2021) Platform competition: A systematic and interdisciplinary review of the literature. *Journal of Management* 47(6): 1528–1563.
- Rodriguez JK, Holvino E, Fletcher JK, et al. (2016) The theory and praxis of intersectionality in work and organisations: Where do we go from here? *Gender, Work and Organization* 23(3): 201–222.
- Rust RT, Kannan PK and Peng N (2002) The customer economics of internet privacy. *Journal of the Academy of Marketing Science* 30(4): 455–464.
- Sannon S and Forte A (2022) Privacy research with marginalized groups: What we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW2): 1–33.
- Schrock AR (2015) Communicative affordances of mobile media: Portability, availability, locatability, and multimodality. *International Journal of Communication* 9: 1229–1245.
- Shifman L (2013) *Memes in Digital Culture*. Cambridge, MA: MIT Press.
- Siddiq F and Scherer R (2019) Is there a gender gap? A meta-analysis of the gender differences in students' ICT literacy. *Educational Research Review* 27: 205–217.
- Steinfeld N (2016) "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior* 55: 992–1000.
- Sthapit E and Björk P (2019) Sources of value co-destruction: Uber customer perspectives. *Tourism Review* 74(4): 780–794.
- Taylor L (2017) What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society* 4(2): 1–14.
- Trepte S, Reinecke L, Ellison NB, et al. (2017) A cross-cultural perspective on the privacy calculus. *Social Media + Society* 3(1): 1–13.
- Turow J, Lelkes Y, Draper N, et al. (2023) Americans can't consent to companies' use of their data: they admit they don't understand it, say they're helpless to control it, and believe they're harmed when firms use their data. *SSRN Electronic Journal*: 1–24. Available at SSRN: <https://ssrn.com/abstract=4391134>
- Tyler TR and Blader SL (2000) *Cooperation in Groups: Procedural Justice, Social Identity and Behavioral Engagement*. Philadelphia, PA: Psychology Press.
- Vaccari C and Valeriani A (2021) *Outside the Bubble: Social Media and Political Participation in Western Democracies*. Oxford: Oxford University Press.
- Van Der Horst H and Messing J (2006) "It's not Dutch to close the curtains": Visual struggles on the threshold between public and private in a multi-ethnic Dutch neighborhood. *Home Cultures* 3(1): 21–37.
- Van Dijck J (2013) *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press.
- Van Dijck J, Poell T and De Waal M (2018) *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press.
- Verswijvel K, Walrave M, Hardies K, et al. (2019) Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. *Children and Youth Services Review* 104: 104401.
- Vitak J, Liao Y, Mols A, et al. (2023) When do data collection and use become a matter of concern? A cross-cultural comparison of US and Dutch privacy attitudes. *International Journal of Communication* 17: 471–498.
- Vitak J, Liao Y, Subramaniam M, et al. (2018) 'I knew it was too good to be true': The challenges economically disadvantaged Internet users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. *Proceedings of the ACM on human-computer interaction*, 2(CSCW), 1–25.
- Walby S, Armstrong J and Strid S (2012) Intersectionality: Multiple inequalities in social theory. *Sociology* 46(2): 224–240.
- West SM (2019) Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society* 58(1): 20–41.
- West SM (2023) Intersectionality and human-machine communication. In: Guzman AL, McEwen R and Jones S (eds) *The SAGE Handbook of Human-Machine Communication*. London: Sage, 342–349.
- Wikipedia (2023) Camden bench. Available at: https://en.wikipedia.org/wiki/Camden_bench.
- Zuboff S (2019) *The Age of Surveillance Capitalism*. New York: Profile Books.
- Zwick D, Bonsu SK and Darmody A (2008) Putting consumers to work: Co-creation and new marketing governmentality. *Journal of Consumer Culture* 8(2): 163–196.