

The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda

Big Data & Society
 January–June: 1–14
 © The Author(s) 2022
 Article reuse guidelines:
sagepub.com/journals-permissions
 DOI: 10.1177/20539517211065368
journals.sagepub.com/home/bds



Moritz Büchi¹ , Noemi Festic¹  and Michael Latzer¹ 

Abstract

People's sense of being subject to digital dataveillance can cause them to restrict their digital communication behavior. Such a chilling effect is essentially a form of self-censorship in everyday digital media use with the attendant risks of undermining individual autonomy and well-being. This article combines the existing theoretical and limited empirical work on surveillance and chilling effects across fields with an analysis of novel data toward a research agenda. The institutional practice of dataveillance—the automated, continuous, and unspecific collection, retention, and analysis of digital traces—affects individual behavior. A mechanism-based causal model based on the theory of planned behavior is proposed for the micro level: An individual's increased sense of dataveillance causes their subjective probability assigned to negative outcomes of digital communication behavior to increase and attitudes toward this communication to become less favorable, ultimately decreasing the intention to engage in it. In aggregate and triggered through successive salience shocks such as data scandals, dataveillance is accordingly hypothesized to lower the baseline of free digital communication in a society through the chilling effects mechanism. From the developed theoretical model, a set of methodological consequences and questions for future studies are derived.

Keywords

Dataveillance, surveillance, chilling effects, self-censorship, privacy, digital communication

Introduction: Sense of Dataveillance and Digital Communication

In the summer of 2020, the president of the United States signed an executive order to suspend temporary work visa renewals (Ordoñez, 2020). A graduate student commented on this news on Twitter, writing that they had wanted to say something about this, but did not, fearing a negative impact on their upcoming visa renewal application. They further wrote, “we should not have to think about these things.” Apparently, a fear of producing digital traces that could have negative repercussions prevented this individual from freely voicing their opinion about a political issue. Judging the potential consequences of one's actions has certainly always influenced people's choices—which is often a desirable outcome—but this example brings out several specificities: The behavior in question, commenting on news online, is mundane and minor; the associated potential consequence, being denied a visa renewal, is far-reaching. The practice of using applicants' digital traces in visa-granting decisions is not transparent. Further, voicing an opinion on government actions is entirely permissible,

regardless of immigration status. As a form of political participation, this behavior is even socially desirable. And, crucially, the reason a possible impact was assumed in the first place is *dataveillance*: the automated, continuous, and unspecific collection, retention, and analysis of digital traces by state and corporate actors. Although it is immediately obvious that the suppression of critical political participation is problematic from a democratic normative stance, the deterrence from routine everyday communication—which today is increasingly mediated by digital media and thus in principle is always traceable—presents an underappreciated risk.

¹Department of Communication and Media Research, Media Change and Innovation Division, University of Zurich, Zurich, Switzerland

Corresponding author:

Moritz Büchi, Department of Communication and Media Research, Media Change and Innovation Division, University of Zurich, Andreasstrasse 15, CH-8050 Zurich, Switzerland.
 Email: m.buechi@ikmz.uzh.ch



This article aims to understand how people's sense of being subject to dataveillance may cause them to restrict their digital communication behavior. This undercuts the vital role accorded to digital communication in contemporary society—potential negative outcomes of digital communication subjected to surveillance may stifle digital media use for everyday activities, personal development, societal participation, or political advocacy. Although these *chilling effects* of dataveillance are thus critical in a digital society, there is only fragmented theory development and at most a handful of studies that have tried to assess chilling effects in the context of dataveillance with various conceptual and methodological limitations. In the specific context of dataveillance of everyday digital communication, chilling effects are here defined as *the self-inhibition of (legitimate) behaviors*, such as expressing one's opinion online (including low-threshold participation like "liking") or searching the web for (sensitive) information. Although in the example above, there is a clear link between the behavior and its potential concrete negative outcome, chilling effects in everyday life will often concern less distinct acts of digital communication and vague assumptions about possible repercussions.

The main contributions of this article are three-fold. First, we develop a theoretical model (integrating insights from media and communication science, law, surveillance studies, and social psychology) focusing on explicit causal mechanisms. Second, we analyze existing empirical studies and original survey data to gauge the magnitude of the chilling effect phenomenon in everyday life. Third, the theoretical model's propositions and empirical findings' limitations are consolidated to demonstrate the requirements for future research. With these three contributions, we hope to motivate a research agenda that will spawn innovative empirical study designs and iterative model revisions aimed at understanding and measuring chilling effects of digital dataveillance.

The System-Level Context of Individual-Level Chilling Effects

Broad dangers of surveillance include discrimination and persuasion (Richards, 2013). Here, we focus on an additional aspect, chilling effects, that has received little attention in the context of dataveillance (Penney, 2017). The potentially harmful consequences of chilling effects for pillars of deliberative democracies, such as freedom of expression, speech, and thought, were recognized nearly half a century ago: individuals who believe they are under surveillance may preemptively self-inhibit free speech and behavior (White and Zimbardo, 1975). In the meantime, fast-growing and ubiquitous dataveillance has severely intensified the problem.

Although the concept of chilling effects goes back even further, articles that rely on a similar definition to the one

used here emerged in the 1970s (Schauer, 1978; White and Zimbardo, 1975) with reference to a 1965 US legal case regarding the free exercise of basic rights. Schauer (1978) argued that errors made in favor of free speech are preferable to the wrongful suppression of free speech. The cause of the chilling effect in this literature was the fear of legal prosecution and the uncertainties of this process. After the September 11 attack, the concept resurged and was applied to counter-terrorism surveillance: Solove (2006, 2007) explicitly introduced surveillance as an inhibitor of people's legitimate activities and acknowledged the indirect nature of the risk. The practice that has a chilling effect, surveillance, is not directed at basic rights in democratic systems, but affects them nonetheless; and Solove (2006) noted that "awareness of the possibility of surveillance can be just as inhibitory as actual surveillance" (p. 495).

In many societies, digital media have become the most convenient means to perform everyday activities such as seeking information or exchanging ideas. Beyond active content creation or "liking" and "following," merely being online produces persistent digital traces and data. The growing collection and analysis of this (big) data (van Dijck, 2014) is automated, continuous, inexpensive, and opaque. It serves corporations to optimize services and profits, and states to ostensibly increase national security. This far-ranging dataveillance system, the systematic monitoring of data reflecting the actions and communication of individuals (Clarke, 1988), may produce a diffuse sense of being constantly watched, potentially deterring people from permitted or even socially desirable behavior. Dataveillance can thereby lead to self-censorship, conformity, and anticipatory obedience. Such chilling effects inhibit the exercising of fundamental rights and consequently constitute a subtle, cumulative risk for individual autonomy, well-being, and democratic participation in digital societies (see Véliz, 2020). Chilling effects are not a uniform or inevitable consequence of dataveillance; some people may alternatively or additionally increase the protection of their data (Chou and Chou, 2021) or engage in *sousveillance* (Mann and Ferenbok, 2013). Chilling effects are one of many processes in a complex system of constantly changing digital communication and are in a sense volatile as well as dependent on further influences, such as dispositions, situations, or type of communication behavior. Our notion of inhibited digital communication behavior certainly includes but is not limited to acts of political participation online—the cumulative effects of undue deterrence from small acts of digital communication to satisfy individuals' personal or social needs in everyday life are just as relevant. Figure 1 provides a rough sketch of individuals' chilling effects in a system-level context. Although there are further links between these elements, this simplified cycle serves to structure the following discussion of relevant concepts.

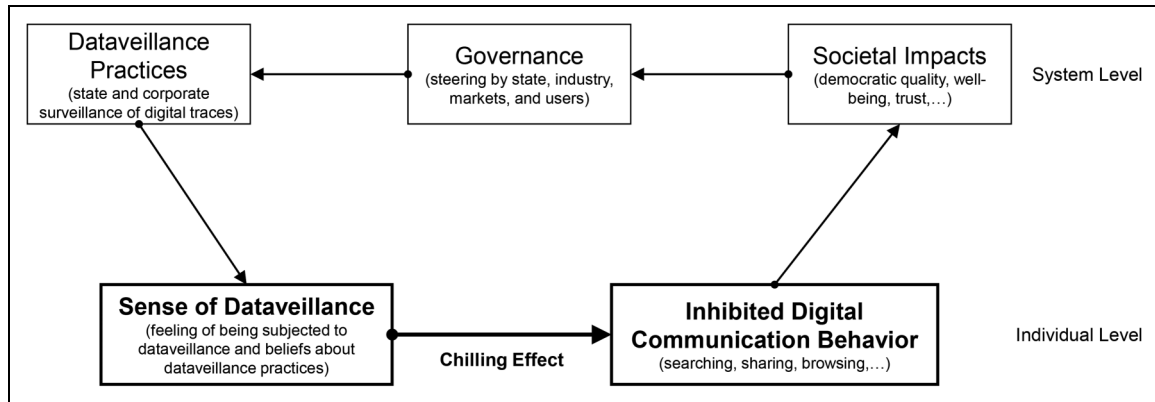


Figure 1. Individuals' chilling effects in a system-level context.

In the early 21st century, the nonstop generation of vast amounts of digital traces related to people's everyday digital communication surged with the establishment of Google, Facebook, and other platform companies. In 2013, documents leaked by Edward Snowden revealed the extent of global dataveillance, yet interest in privacy and self-protection in everyday digital media use was short-lived (Preibusch, 2015). The more subtle, longer term consequences have only recently been recognized with the concept of chilling effects in light of dataveillance, and empirically with studies by Penney (2016) on Wikipedia, Marthews and Tucker (2017) on Google Search, and Stoycheff (2016) on Facebook. The focus has been on state surveillance and intelligence agencies, yet people are increasingly confronted with negative outcomes due to corporate (Noble, 2018) or state–corporate partnership (Schneier, 2013) dataveillance.

Our model is developed from the perspective of a liberal democracy where digital communication is ubiquitous in everyday life. Yet the chilling effects mechanism may likely be more evident and less subtle in countries with weaker protection of free speech and more authoritarian governments, where for example, the use of virtual private networks is banned or providers of messaging apps have to identify their users (Bakir, 2021).

Societal Impacts and Governance

The isolated chilling effect results in the suppression of behavioral intention. The *antecedents* of this process are actual dataveillance practices and societal governance arrangements that enable or constrain dataveillance practices (see Figure 1). The *consequences* of the chilling effect manifest in individuals' behaviors, which in aggregate lead to societal impacts, for example, an increase in conformity and less inclusive democratic processes. Deterrence from participating in democracy's requisite debates impedes the deliberative process "aimed at producing reasonable, well-informed opinions in which

participants are willing to revise preferences in light of discussion, new information, and claims" (Chambers, 2003: 309). These consequences, for example, then prompt regulatory responses by states or users' self-help strategies as a form of governance that may be supported by public policy. The current state of research in the field has either focused on the macro-level ethical implications of surveillance (e.g. pointing to very general risks and long-term implications for a liberal society, see Citron and Gray, 2013) or analyzed rather isolated instances of microlevel behavioral adaptations (e.g. a decrease in online self-disclosure, see Dienlin and Metzger, 2016). A lack of transparency and control over how dataveillance effectively functions and its gradual normalization lead to feelings of resignation despite unease. This may impede collective action that would engender alternative ways of governing digital communication, leaving only the option to pragmatically adapt individual behaviors (see Dencik and Cable, 2017; Hoffmann et al., 2016; Smith, 2018). Governance alternatives should no longer assume that individuals are in a position of control to make informed choices according to their preferences for trading personal data for benefits they receive (Draper, 2017). Individuals who are aware of the massive dataveillance apparatus may care a great deal about negative consequences, yet feel powerless and the consequential "decision not to engage may be a justifiable act of self-preservation" (Draper and Turow, 2019: 1828).

In societies where the (dataveilled) use of digital media is de facto non-optional for everyday functioning, such chilling effects on digital communication, including but not limited to exercising fundamental rights, may be a long-term and cumulative risk for individual autonomy and collective action, warranting further academic attention. A holistic perspective on chilling effects, therefore, includes a macro perspective on the governance arrangements that steer dataveillance practices as a response to the societal risks of inhibited digital communication. Individuals in a specific population will vary greatly in their general preferences regarding digital communication and in their

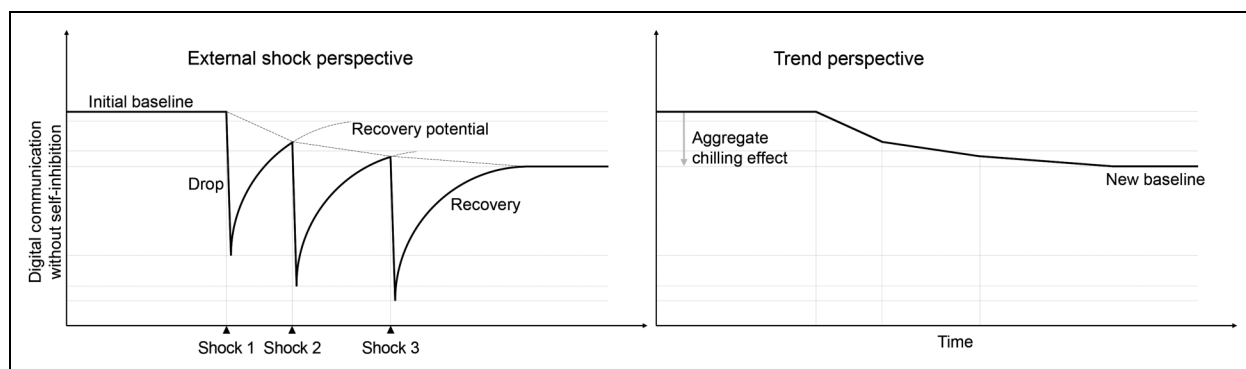


Figure 2. How imperfect recovery from shocks may lead to long-term chilling of digital communication.

responses to an increased sense of dataveillance. Nonetheless, a population or social system can be characterized by its average level, or baseline, of digital communication without self-inhibition; communication regarded as normatively desirable in the social system (i.e. “non-chilled”) (Figure 2). An exogenous event, or shock, that makes dataveillance salient is expected to cause a relatively sudden drop in this digital communication. The magnitude of this drop will depend on the specifics of the shock such as the breadth and severity of the dataveillance practice revealed. Typically, drastic self-inhibition in the immediate aftermath of a shock characterized by extreme uncertainty regarding personal affectedness will quickly subside (see Preibusch, 2015) and a “back to normal” recovery phase ensues. Any lasting effect, for instance, a minor overall decrease in the level of expressing personal views through digital communication, indicates an incomplete recovery, and over time, a trend to a new baseline (equal to the initial baseline minus the sum of unrecovered digital communication across all shocks). The denser the succession of shocks, the more overall chilling occurs as subsequent self-inhibition interrupts the previous recovery phase. This temporal accumulation of short-term chilling effects to long-term risk is loosely inspired by excitation transfer theory—a model of emotional reactivity where residual excitation from preceding experiences carries over (see Zillmann, 2008; Zillmann et al., 1972)—and Hebbian theory—a biological learning mechanism where a repeated activity induces lasting change at the level of neurons (Galluppi et al., 2015; see Suri, 2004).

Current discussions surrounding technological solutions to contain the spread of COVID-19 illustrate the broader societal issues of dataveillance: shortly after drastic lockdown measures were implemented across the globe in early 2020, a plethora of countries launched tracing apps and other health-based surveillance technologies (e.g. thermal scanners) as promising measures against an uncontrollable spread of the virus (Chiusi et al., 2020). Objecting institutions and actors raised concerns—accusing governments of technological solutionism (see Morozov,

2013) and fearing a long-term normalization of mass surveillance (Chiusi et al., 2020) with potentially unforeseen effects—especially since the effectiveness of these measures was not proven. At the core of this conflict of interests is the pursuit of a balance between public safety (including health) and individual autonomy (see e.g. Broeders et al., 2017; van Brakel, 2016). This discussion also shows the popular opinion that even if such tracing apps do not achieve their stated purpose (i.e. containing the spread of the virus), they at least “do no harm.” Potential subtle, long-term effects of such dataveillance practices on communication behavior—as described by the chilling effects literature—often remain invisible (see Vitak and Zimmer, 2020).

In the aftermath of data scandals or personal negative experiences, the focus is on the immediate reaction, which may be substantial self-inhibition, but this effect tends to dissipate over time. We propose, however, that this recovery is likely to be incomplete, particularly as reports and public awareness about dataveillance are intensifying, imperceptibly leading to a lower societal level of “normal,” unrestricted digital communication (see Figure 2). Although the focus here was on shocks like data scandals that generally induce negative outcomes for individuals, in principle, appropriate governance mechanisms could invert the plotted trajectory and cause an *increase* in digital communication without self-inhibition. For example, the idea of a small “data tax” on companies (e.g. data brokers) as a fiscal incentive to collect less data has been discussed (Madsbjerg, 2017). The right mix of public and private contributions to a governance arrangement (Latzer, Saurwein, et al., 2019) can play a key role in the relationship between dataveillance, individual digital communication, and societal impacts (Figure 1).

The societal relevance of contemporary dataveillance leading to chilling effects lies in the “lost potential” of digitization and the internet: the uninhibited flow of human knowledge is *technically* possible, yet due to its sociopolitical domestication into existing power structures, the past decade has shown a turn away from the liberatory and participatory potential (see, e.g. Benkler, 2007; Friedewald

et al., 2010; Hilbert, 2020; Schradie, 2020). “The revolution that wasn’t” (Schradie, 2019) is in the process of negating the promise of the internet to promote human flourishing —“putting people first, promoting democracy, and protecting them from exploitation and vulnerability” (Richards and Hartzog, 2020: 66), with people seemingly content with minor benefits such as relevant ads. Legal scholars point out that regulation (or nonregulation) directed toward dataveillance needs evidence on why and under which conditions surveillance is actually harmful in terms of basic rights (Richards, 2013); particularly, empirical studies on the idea that “surveillance deters the kinds of activities and communications necessary for people to lead full lives as individuals and democratic citizens” (Sklansky, 2014: 1095) are strikingly scarce. As a central but underappreciated risk of surveillance, chilling effects require further theoretical and empirical research to assess the impact of the current system of dataveillance on uninhibited everyday digital communication, a crucial resource for individuals’ well-being (see Segrin, 2014).

Dataveillance Practices and People’s Sense of Dataveillance

The amount of data on individuals’ lives that is generated and can be collected and analyzed has tremendously increased as a result of digitization. In digitized societies, digital services are often the most convenient and effective way to perform everyday tasks. This includes the mundane, such as looking up directions on Google maps, watching a Netflix series, talking to friends on Facebook Messenger, or buying products online. Higher involvement activities such as researching health information, professional collaboration, or political expression are often enabled by the same devices, services, and platforms. The result is that these diverse communication behaviors leave digital traces, that is, they have become datafied (van Dijck, 2014; Ytre-Arne and Das, 2021).

The stated corporate interests in dataveillance are, for example, maximizing user engagement and influencing behavior through the personalization of ads, search results, and recommendations (e.g. Boerman et al., 2017; Esposti, 2014); on the part of government-led dataveillance, public safety is generally cited, ostensibly achieved through counter-terrorism activities and predictive policing based on digital traces (e.g. Andrejevic, 2017; Lyon, 2014). Over the past couple of years, through Snowden’s NSA revelations in 2013, the Cambridge Analytica case in 2018 (Cadwalladr and Graham-Harrison, 2018), and lesser scandals, everyday users of internet-based technologies have become increasingly aware that they are being constantly tracked. These data are used detached from context, combined with data from other users, and analyzed in ways that the individual has no control over. With the outbreak of COVID-19, in a very short time, this system

of dataveillance has broadened in scale and scope to additional forms of data collection such as thermal scanners, GPS-based location services, and facial recognition systems, imposing “a new normal” based on pervasive and health-based surveillance (Chiusi et al., 2020).

This dataveillance here refers to surveillance, that is, “the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction” (Lyon, 2007: 14) but based on digital traces. The critical shift lies in its automation, making dataveillance attractive for businesses and governments even when there is no “suspicion” or immediate purpose, “just in case.” The lower cost per unit, remoteness, lower visibility, and continuous real-time nature facilitate these practices (see Clarke, 1988; Marx, 2002; van Dijck, 2014). Dataveillance may be very broad, including all types of sensors and data related to different entities; of primary interest here is the subtype of profiling automated by algorithms as the “recording and classification of data related to individuals” (Büchi et al., 2020: 2).

Although particularly the field of law and emerging surveillance studies have initiated the discussion related to basic rights like freedom of expression, there is a distinct lack of theory on the contributing factors to chilled, or inhibited, general digital communication that would propose clear hypotheses for empirical examination. The current consensus in the literature is merely that chilling effects are a “potential danger” of surveillance, subject to empirical confirmation. Drawing on the extant literature that has intersected with digital communication behavior (e.g. Penney, 2016), we propose that, at the individual level, a sense of dataveillance is the dominant cause of communicative *inhibition*, that is, the relevant chilling effect lies in this link. For individuals, the situational and long-term varying sense of dataveillance is partly exogenously influenced, for instance, through public scandals, but also affected by personal uses, skills, and experiences, such as realizing that previously used search terms lead to very specific ads, even on different platforms or devices (Tanner, 2015). Practices such as audio watermarking and IP matching invoke high levels of perceived surveillance, whereas demographic segmentation based on social media data is viewed as less problematic by users (Segijn and van Ooijen, 2020). In the context of smart home devices, Frick et al. (2021) found that trust in the devices’ handling of client data, general anxiety toward computers and automation, and prior negative experiences predicted perceived surveillance of conversations, that is, that the smart device secretly listened in, and suggest that perceived sensitivity of the content should additionally be examined. Confronted with information about or indications of dataveillance practices, whether factually correct or not, this elevated cognitive availability (“top of the head” phenomenon; Taylor and Fiske, 1978) will tend to play a more important role in the formation of subsequent digital communication

behaviors (see Trepte, 2021). Additionally, personal vulnerability because of an increased risk of discrimination for certain social identities (see Matzner et al., 2016), or the presumed magnitude of repercussions may also inhibit digital communication.

Inhibited Digital Communication Behavior

After having situated chilling effects in a system of data-veillance practices arguing that the cause of long-term shifts in digital communication is affected by exogenous shocks, we zoom in on the individual level process of self-inhibition, which is where the main contribution of this article lies. Ytre-Arne and Das (2021) suggest that people “often know that their engagements leave traces that form patterns and feedback loops, but also that the full extent of these are beyond transparency, rendering the prediction of outcomes of communicative exchanges less apparent” (p. 14). Thus, while day-to-day routines do not constantly foreground potential negative outcomes, data scandals, and other salience shocks “remind” people of the extensive practice of dataveillance. An expected reaction to an increase in awareness to this massive system of dataveillance is self-restraint in order to increase conformity with perceived societal norms (e.g. Manokha, 2018): a chilling effect, which can also be understood as anticipatory obedience or self-censorship. This deterrence from or suppression of (legitimate) behavior existed long before digital technologies came to fundamentally pervade all domains of everyday life in modern societies (White and Zimbardo, 1975) but has attained new significance in light of dataveillance. If people know they are being watched—or believe they know, regardless of the factual extent of dataveillance—this can deter them from exercising permitted or even socially desirable behavior. This behavioral modification occurs without the state or corporations ever directly exerting power (see e.g. Büchi et al., 2020; Marthews and Tucker, 2017; White and Zimbardo, 1975), making chilling effects a latent and subtle process, and thus potentially under-acknowledged as a risk.

The internet and the digital media based on it are uniquely predisposed to serve information seeking and self-expression, yet pervasive, indiscriminate dataveillance through the algorithmic construction of personal data profiles may suppress these practices (see Büchi et al., 2020; Friedewald, 2018; Hildebrandt, 2008). Many potentially chilled behaviors have received very little attention due to their seeming mundaneness. Yet everyday behaviors such as researching a contentious or an entirely noncontroversial topic online, sending messages on a smartphone, or liking other people’s posts on social networking sites make up the fabric of social life in the digital society. The hypothesis in the existing research is that surveillance acts as a normalizing gaze (Richards, 2013) upon these activities, a sense of

being watched and judged, that suppresses “experimentation with the unorthodox” (Cohen, 2000: 1426).

The imprecise but perhaps intuitive formulation of the chilling effect hypothesis in the existing research is that *an increase in dataveillance practices inhibits digital communication*. Or, as stated above, at the individual level a subjective sense of dataveillance, dependent on the objective dataveillance practices, causes the communicative inhibition. But how exactly does this link work? For a precise explication, we base the “chilling effect proper” on the social-psychological theory of planned behavior (TPB; Ajzen, 1991), which has been widely applied in research on behavioral adaptations, including digital technology use (Ajzen, 2020). Embedded in a broader logic (see Figure 1), chilling effects themselves are an individual-level process of action formation, thus the general TPB can be productively applied: “At the most basic level of explanation, the theory postulates that behavior is a function of salient information, or beliefs, relevant to the behavior” (Ajzen, 1991: 189). TPB posits that the immediate cause of a behavior, such as digital communication, is the intention to engage in said behavior; the proximal determinants of this behavioral intention are the attitude toward the behavior, subjective norms pertaining to the behavior, and perceived ability to perform the behavior.

The sense of dataveillance will primarily affect the person’s attitude toward digital communication (see Bräunlich et al., 2021)—basically, the individual’s evaluation of whether digital communication, and thus leaving digital traces, is “a good idea”—this evaluation need not be extensively processed cognitively. More technically: “attitude toward the behavior is assumed to be a function of readily accessible beliefs regarding the behavior’s likely consequences” (Ajzen, 2020: 2). This is the “point of entry” of dataveillance practices into individuals’ communication behaviors (see Figure 3): an increase in dataveillance salience, such as through news reports, is expected to heighten people’s sense of dataveillance and thereby the accessibility of the belief that digital communication behavior can entail personal repercussions (negative outcomes), which would make the attitude toward the behavior less favorable, which then decreases the intention to engage in the behavior.

A number of mediating and moderating processes are predicted by TPB—applied to dataveillance and digital communication, the most likely source of observing differential effects of dataveillance salience on inhibited digital communication behavior are background factors (sociodemographics, personality, values, etc.). For instance, noncitizens may be much more wary of researching or posting content critical of the government. Further, “algorithmic profiling that facilitates the inclusion of different sources and types of data is likely to contribute to increasing entanglements of protected identities, thus creating new categories and groups of people that experience forms of intersectional discrimination” (Mann and

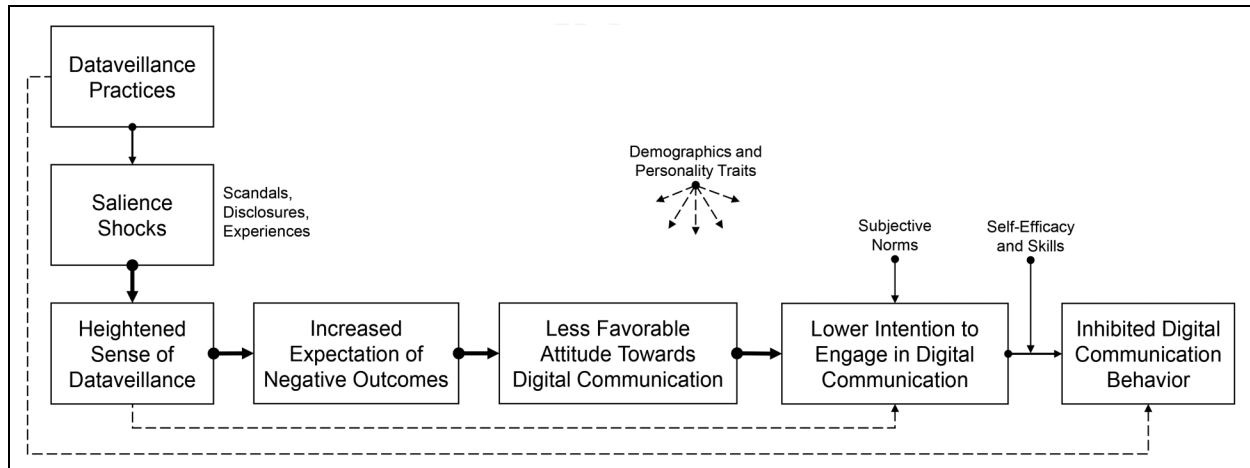


Figure 3. Mechanisms of the chilling effect of dataveillance practices on digital communication.

Matzner, 2019: 5)—individuals potentially affected by such discrimination may justifiably form beliefs of negative outcomes, which mediate how the sense of dataveillance ultimately impacts digital communication. Salience shocks, for example, through media reports or negative experience, will on average increase the level of perceived dataveillance, but there will be qualitative differences in how people update their conceptions of how dataveillance works (Ytre-Arne and Moe, 2021). The more dataveillance is attributed to human or human-like actors, the higher the individual susceptibility to chilling effects (Festic, 2020; Siles et al., 2020).

Applying TPB, the behavior of interest is here defined as engaging in digital communication that produces digital traces in everyday life—for example, for the purpose of information-seeking, self-expression, social coordination, or entertainment. Consequently, the other elements of the mechanism (see Figure 3) are defined in relation to this behavior of interest. We accordingly formulate the general, isolated chilling effect hypothesis as a microlevel causal mechanism triggered by an external factor.

Chilling effect of dataveillance hypothesis: An increased sense of dataveillance causes individuals' subjective probability assigned to negative outcomes of digital communication behavior to increase and attitudes toward this communication to become less favorable, decreasing the intention to engage in it.

Toward an Empirical Test of Chilling Effects

Insights From and Gaps in Existing Studies

Assessing the prevalence of chilling effects and the necessity for governance interventions requires a solid empirical basis. The most critical issue in the current state of research in the field is that there is overall extremely limited

empirical research. Studies on the chilling effects of dataveillance have only been prompted very recently by the revelations surrounding the NSA's surveillance practices (Penney, 2016). In addition to a few qualitative studies that incidentally touch on chilling effects (e.g. Lupton, 2020), there is a very limited body of quantitative research in the field.

In an experimental study, Stoycheff (2016) surveyed 255 US participants in an online questionnaire with a priming manipulation in a Facebook post: those who were primed that their social media usage would be surveilled, and who had opinions diverging from the mainstream regarding US airstrikes on ISIS, were particularly likely to be deterred from posting their opinions. In addition to a concern of being socially isolated, Stoycheff (2016) suggests fear of prosecution by the government as a plausible contributor. However, a precise mechanism and externally valid setting are needed. Further, the role of direct and indirect negative outcomes due to corporate dataveillance has not been considered, especially empirically. In another experimental setting, Stoycheff et al. (2019) found that higher perceived online government surveillance chilled not only participants' likelihood to engage in illegal activities online but also deterred intentions to engage in legitimate political activities online (e.g. sharing opinions, criticizing the government). This effect was found both for a demographically diverse sample and a group of adults who identified as Muslim.

In addition to these experimental studies, there have been attempts to measure chilling effects in cross-sectional observational or survey research. To the best of our knowledge, all existing observational studies rely on the NSA revelations as a natural stimulus. An innovative study on Wikipedia use analyzed how web traffic to privacy-sensitive articles (e.g. Al Qaeda, Iraq, Nationalism) changed after the publicization of NSA surveillance (Penney, 2016). The main finding was that traffic to these

articles immediately and significantly declined after the revelations—although clearly, reading up on any of these topics is entirely legitimate citizen behavior. In a very similar manner, Marthews and Tucker (2017) compared the search volume of selected privacy-sensitive keywords on Google in 11 countries before and after the NSA surveillance revelations. They found significantly lower traffic for search terms of which the participants were concerned that they could get them in trouble with the US government (e.g. Chemical Spill, Explosion, Tuberculosis) after the 2013 surveillance disclosures. On an international scale, Google users were also found to be less likely to use search terms that they perceived as potentially sensitive (e.g. Atheism, Herpes, White Power). Also at the aggregate level of search volume, Rosso et al. (2020) found a significant and lasting increase in the use of the DuckDuckGo search engine (whose unique value proposition is to not profile its users) directly following the NSA revelations.

A large survey in Norway also addressed this topic and indicated the existence of significant chilling effects on online behavior. In 2014, significant proportions of the Norwegian population indicated having decided to not make a purchase (28%), to not sign a petition on the internet (26%), or to talk face-to-face rather than communicate electronically (26%) because they were unsure how such digital traces would be used in the future (Teknologirådet and Datatilsynet, 2014). The results also revealed that many would be more careful about their online searches (27%) or their posts (24%) if intelligence services were to surveil their everyday internet use (Teknologirådet and Datatilsynet, 2014). The results from the 2019 wave were very similar, revealing chilling effects due to government surveillance regarding looking for information about sensitive topics and expressing opinions online; chilling effects on digital communication behavior due to concerns about how private companies use their data appeared to be even more pronounced (Datatilsynet, 2020).

Indications of Widespread Chilling Effects

This article developed a theoretical model connecting dataveillance and inhibited digital communication (see Figure 3). Before attempting a comprehensive empirical test thereof, we need to know whether there is good reason to assume that chilling effects are a part of everyday internet use for a substantial number of people in the first place. To initially assess the magnitude of the phenomenon, we included several questions in large-scale surveys. An initial result was that more than half of internet users felt dataveillance deterred them from self-expression or information seeking, ranging from rarely to always; chilled self-expression was substantially more frequent than chilled information-seeking (Lutzer, Büchi, et al., 2019). Here, we report additional original results from a second, dedicated and more detailed dataveillance survey module

within a research project in Switzerland that investigates the role of algorithms in everyday life in a population-level sample (Lutzer, Festic, et al., 2020). The sample of 1202 respondents is representative of age, gender, region, household size, and employment status for internet users aged 16 and over. Respondents were sampled by an independent social and market research company, and the online questionnaire was fielded in three languages between late 2018 and early 2019.

The items were introduced by stating that the interest was in whether respondents adapted their online behavior to potential risks. It was necessary to include the behavior in question (e.g. information seeking) and a cue to dataveillance in a single item as not to displace reports of subtle self-inhibitions by more prominent reasons for certain communication behaviors (e.g. simply not being interested in a topic and thus not seeking information about it). The four statements relate to *being cautious* (“I believe one is constantly surveilled on the internet, therefore I am cautious in my online behavior”), *avoiding attention* (“I try to avoid attention on the internet because of the vast surveillance possibilities”), *inhibiting opinion sharing* (“I do not always share my opinion online, because such data traces on the internet could harm me”), and *inhibiting information seeking* (“I do not seek information about certain topics online because such data traces on the internet could harm me”). Insofar as establishing a causal link (“therefore,” “because”) between digital communication behaviors and dataveillance can be delegated to respondents, the results indicated potential chilling effects: Combining response values 4 and 5, between 20% (inhibiting information seeking) and 45% (inhibiting opinion sharing) reported agreement (see Figure 4). Considerable numbers of the internet user population reported self-inhibition with regard to these entirely legitimate uses of the internet.

Overall, the reported experiences of chilling effects due to dataveillance appear relatively similar across major sociodemographic groups (see Figure 5), particularly considering that many practices and attitudes related to internet use exhibit significant variation across age and sex (Lutzer, Büchi, et al., 2020). Within age groups, the only significant (i.e. where the confidence intervals do not overlap) sex difference in the chilling effects indicators concerned opinion sharing: on average, women aged 60 to 79 were more likely to self-inhibit this digital communication behavior than men of the same age. In general, younger internet users tended to report smaller chilling effects, but differences are in the realm of no more than half a point between the youngest and oldest age groups on the 1 to 5 scale.

Consequences for Further Research

Although there is evidence for the existence of chilling effects in the context of dataveillance—both from existing research and the new data provided here—the empirical

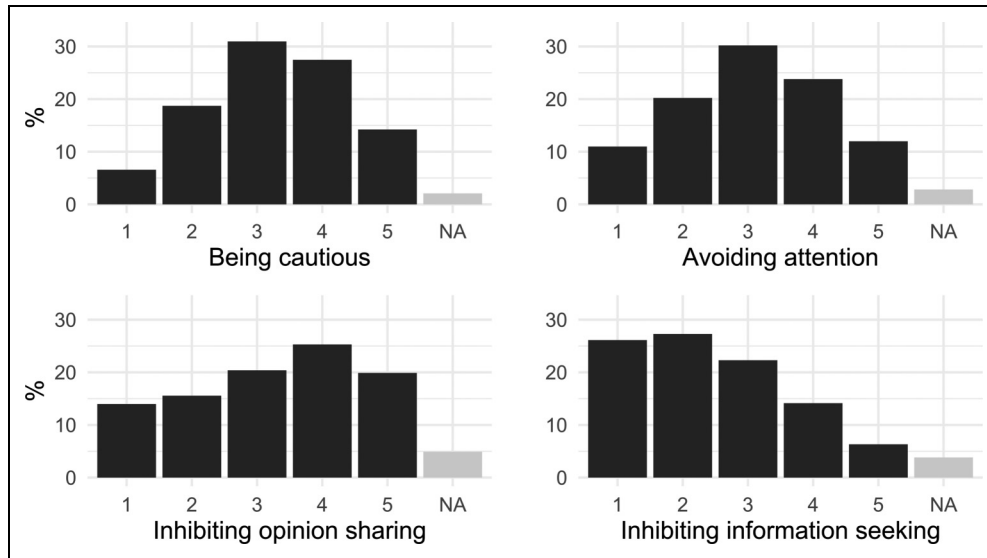


Figure 4. Indicators of chilling effects distributions. Note. Items were worded so that higher values indicate stronger chilling effects (NA reflects non-response and “don’t know” answers). Respondents reported their agreement with four statements suggesting dataveillance as a cause of certain behaviors.

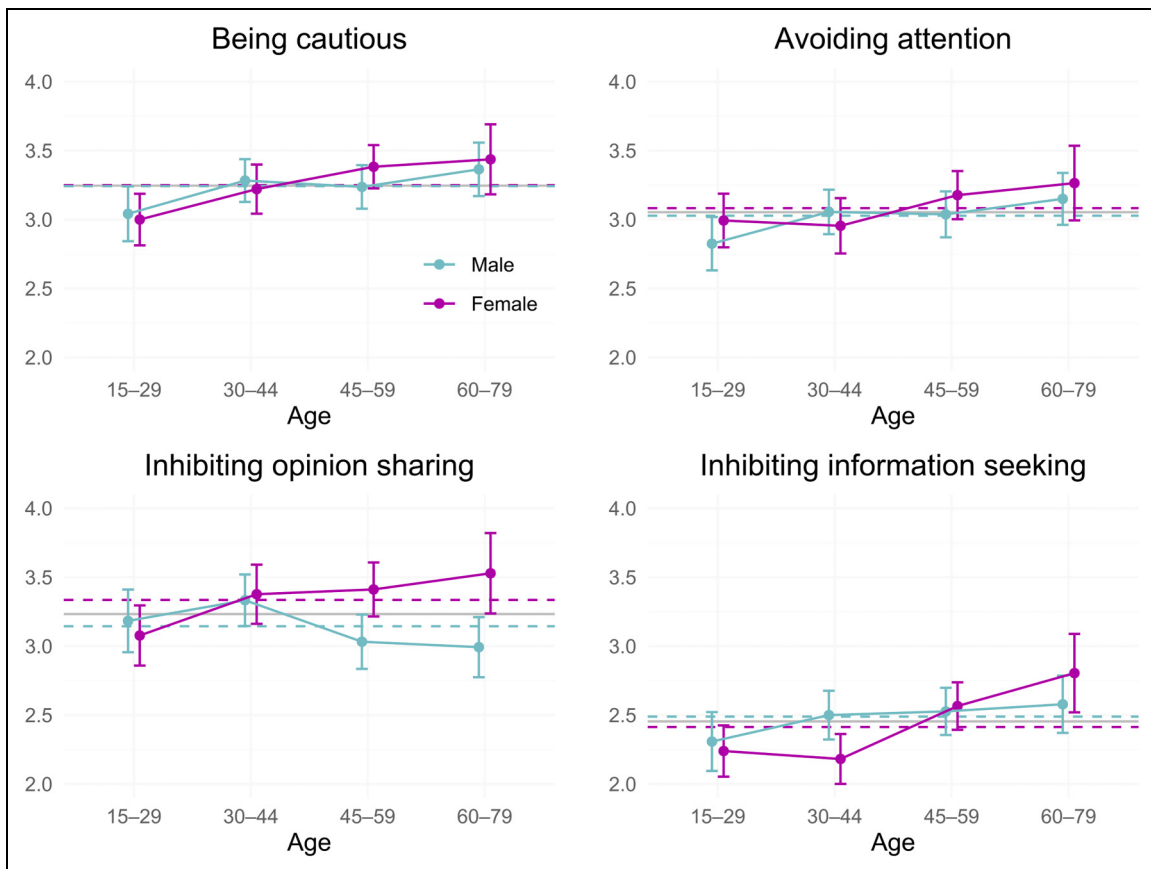


Figure 5. Indicators of chilling effects by age and sex. Note. Vertical bars represent 95% confidence intervals; horizontal lines represent overall (solid) and group means (dashed). Y-axis indicates means on a discrete scale: 1 “do not agree at all” to 5 “strongly agree.”

study designs have not been able to provide robust accounts of actual chilling effects. The general lack of empirical studies is presumably and partially due to disciplinary roots in law, where empirical research is comparably rare, as well as its only recent adaptation to the specifics of dataveillance as opposed to “traditional” surveillance. Moreover, the chilling effects hypothesis has a few inherent characteristics that make it difficult to test empirically (Table 1).

Empirical study designs will need to combine the strengths of multiple complementary methods listed in Table 1, but many difficulties remain as employing one measurement strategy may impinge on the feasibility of another. An experimental component, where participants are randomly assigned to conditions—for example, with varying intensities of (manipulated) sense of dataveillance and a control group—would allow strong conclusions on the causality of chilling effects. This set-up, however, would need to be implemented not in a lab but in situ to

Table 1. Current challenges and recommendations for further research.

Methodological/theoretical challenge	Recommendation
Cross-sectional findings lack validity because chilling effects are conceptualized as long-term.	Employ longitudinal designs, in particular intensive longitudinal methods (Hamaker and Wichers, 2017) as typical two- or three-wave panel designs will likely not capture the effect.
The causal effect of an increased sense of dataveillance cannot be strongly supported without a control group.	Integrate experimental components into study designs to manipulate the sense of dataveillance.
Expected effect sizes are very small because chilling effects are conceptualized as subtle.	Measure digital communication behavior with unobtrusive strategies such as technology-assisted reconstruction (Karapanos, 2020) and log data (Christner et al., 2021).
Wordings that accurately convey the chilling effects phenomenon to lay people as survey participants are lacking.	Develop items with qualitative interviews (questionnaires can complement observational methods).
Studies relying (solely) on self-reports lack validity because of recall bias and hypothetical scenarios, and people may not be aware of being affected by chilling effects.	Measure sense of dataveillance and digital communication behaviors close to when they occur in everyday life using in situ assessment methods (Doherty et al., 2020).
State and corporate dataveillance practices and other macro-level variables have low variance and cannot be manipulated.	Test possible changes in dataveillance practices and regulations with simulation approaches (Lempert, 2002).

ensure external validity. To this end, techniques of ecological momentary assessment such as smartphone-based mobile experience sampling could be adopted (see Doherty et al., 2020; Kubey et al., 1996; Schnauber-Stockmann and Karnowski, 2020). Even in a large-scale mixed-method study along these lines, many exogenous factors relevant for different manifestations of chilling effects would remain unaccounted for. Here, simulation approaches can provide further insights, for example, through agent-based modeling (see Bruch and Atwell, 2015; Epstein, 1999; Jackson et al., 2017). In an empirical investigation in a relatively stable social system, the level of perceived legitimacy of dataveillance will not vary considerably, yet this variable can be targeted by regulations and policies. A simulation can artificially vary relevant variables with low practical variance even in long-term studies, such as regulations, to predict the effects they may have on behaviors. As we introduce more variables, empirical tests of all possible combinations of these variables are increasingly unfeasible, but simulations can easily experiment with this “behavior space” and point to likely or interesting cases that warrant an empirical test. Finding a mix of theoretically appropriate and feasible methods remains challenging because all the above approaches again entail challenges. Researchers will perhaps need to delimit a manageable part of the full model (Figure 3) and balance different methods’ strengths and weaknesses with available resources.

Most importantly, the lack of and shortcomings of empirical studies first call for further theoretical specification of the connection between dataveillance and inhibited digital communication behavior—an endeavor for which we hope to have laid the foundation. If researchers know exactly what they are looking for, they will be more likely to find it and derive relevant conclusions, not least for governance options—or, if findings are inconsistent with the theory, at least have greater confidence in the true absence of the effect.

Conclusion

People’s sense of being subject to digital dataveillance can cause them to restrict their digital communication behavior—such a chilling effect is a self-inhibition in everyday digital media use with the attendant risks of undermining individual autonomy, well-being, and democratic participation. There is evidence of chilling effects—both from existing studies and the new data provided here, yet a robust validation requires further empirical research. The framework presented provides the underlying causal model that unpacks the process between individuals’ sense of dataveillance and their digital communication behavior.

Several theoretical and empirical gaps remain; the following questions may present productive avenues for future research regarding the scope, process, prevalence, and governance of the chilling effects of dataveillance:

- *Scope*: Do users consciously experience chilling effects? What everyday digital communication behaviors are most affected? Where and when do users notice being subjected to dataveillance? How are specific demographic groups differentially affected by chilling effects?
- *Causal process*: Does an exogenous shock such as news of a data scandal heighten people's sense of dataveillance and decrease their intention to engage in unrestricted digital communication? What is the magnitude of people's behavioral adaptation? What factors intervene in this process (e.g. personality traits)?
- *Prevalence*: How prevalent are the "variants" of chilling effects (regarding state vs. corporate, different types of communication) and attitudes toward associated personal and societal risks? Which background variables (e.g. digital skills, sociodemographic attributes) explain differential experiences of chilling effects?
- *Governance*: What harms do users see arising from self-inhibited digital communication? What are likely effects of different, potentially extreme dataveillance practices or regulatory choices on chilling effects?

The outlined theory of the chilling effects of dataveillance does not suggest that entirely uninhibited digital communication is a silver bullet for democracy or that the things people search for or post online should never have consequences. Rather, such consequences need to be reconciled with people's expectations of privacy and their commensurability. In the example in the introduction, a proportionate consequence of expressing one's—in this case presumably strongly opposing—views on the suspension of visa renewals would be that someone else replies with a strongly supporting opinion. If the first person then in the future chooses to not express their views on such topics because the confrontation was experienced as negative, this is not problematic; however, the automated collection of such digital traces and compiling them into data profiles for any use in the future, out of context, and without the knowledge of the data subject is a threat to autonomy and democratic processes (Büchi et al., 2020; Hildebrandt, 2008; Mann and Matzner, 2019; Wachter and Mittelstadt, 2019; Wright and Raab, 2014). We have provided an initial model of how this dataveillance inhibits individuals' digital communication behavior which can inform empirical research designs and further theoretical development.

In the greater context of the impact of the internet on society, chilling effects are one process among countless; analytically isolating this mechanism has been the goal of this article. Dataveillance can suppress political voices, but at the same time, democracy does not require the most open form of communication—in particular when online communication merely forestalls "real antagonism" (Dean, 2005). But beyond political behavior, the urgency of studying the chilling effects of dataveillance lies in digital communication's role in daily life: internet use is a

valuable resource in fulfilling everyday needs such as information, interaction, transaction, or entertainment. Fear of undue negative consequences from useful and legitimate digital communication need not be added to the list of existing digital inequalities (Van Dijk, 2020). The deciding factor in researching a topic or talking to someone online, offline, or not at all should not be driven by the fear of being profiled in the case of choosing the online option.




Declaration of conflicting interests

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

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Schweizerischer Nationalfonds zur Förderung der Wissenschaftlichen Forschung (grant number 176443).

ORCID iDs

Moritz Büchi  <https://orcid.org/0000-0002-9202-889X>
 Noemi Festic  <https://orcid.org/0000-0002-3918-3639>
 Michael Latzer  <https://orcid.org/0000-0003-1237-8863>

References

- Ajzen I (1991) The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50(2). Theories of Cognitive Self-Regulation: 179–211.
- Ajzen I (2020) The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*. DOI: 10.1002/hbe2.195.
- Andrejevic M (2017) Digital citizenship and surveillancel To Pre-empt a thief. *International Journal of Communication* 11: 879–896. Available at: <https://ijoc.org/index.php/ijoc/article/view/6308> (accessed March 14, 2019).
- Bakir V (2021) Freedom or security? Mass surveillance of citizens. In: Ward SJA (ed.) *Handbook of Global Media Ethics*. Cham: Springer International Publishing, pp. 939–959. DOI: 10.1007/978-3-319-32103-5_47
- Benkler Y (2007) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. 9/23/07 edition. New Haven, London: Yale University Press.
- Boerman SC, Kruikemeier S and Borgesius FJZ (2017) Online behavioral advertising: A literature review and research agenda. *Journal of Advertising* 46(3). Routledge: 363–376.
- Bränlich K, Dienlin T, Eichenhofer J, et al. (2021) Linking loose ends: An interdisciplinary privacy and communication model. *New Media & Society*: 23(6): 1443–1464. DOI: 10.1177/1461444820905045
- Broeders D, Schrijvers E, van der Sloot B, et al. (2017) Big data and security policies: Towards a framework for regulating the phases of analytics and use of Big data. *Computer Law & Security Review* 33(3): 309–323.
- Bruch E and Atwell J (2015) Agent-based models in empirical social research. *Sociological Methods & Research* 44(2): 186–221.

- Büchi M, Fosch-Villaronga E, Lutz C, et al. (2020) The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review* 36: 105367.
- Cadwalladr C and Graham-Harrison E (2018) Revealed: 50 million Facebook profiles harvested for Cambridge analytica in major data breach. *The Guardian*, 17 March. Available at: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (accessed September 25, 2020).
- Chambers S (2003) Deliberative democratic theory. *Annual Review of Political Science* 6(1): 307–326.
- Chiusi F, Fischer S and Spielkamp M (2020) *Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective*. AlgorithmWatch, Bertelsmann Stiftung, Berlin, Germany. Available at: <https://algorithmwatch.org/wp-content/uploads/2020/08/ADM-systems-in-the-Covid-19-pandemic-Report-by-AW-BSt-Sept-2020.pdf>
- Chou H-L and Chou C (2021) How teens negotiate privacy on social media proactively and reactively. *New Media & Society*. SAGE Publications: 14614448211018796. DOI: 10.1177/14614448211018797
- Christner C, Urman A, Adam S, et al. (2021) Automated tracking approaches for studying online media use: A critical review and recommendations. *Communication Methods and Measures* 0(0). Routledge: 1–17.
- Citron DK and Gray D (2013) Addressing the harm of total surveillance: A reply to professor Neil Richards. *Harvard Law Review* 126(32): 262–274. Available at: <https://core.ac.uk/download/pdf/56355611.pdf>
- Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512.
- Cohen JE (2000) Examined lives: Informational privacy and the subject as object. *Stanford Law Review* 52: 1373–1438.
- Datatilsynet (2020) *Personvernundersøkelsen 2019/2020*. Datatilsynet—The Norwegian Data Protection Authority, Datatilsynet, Oslo, Norway. Available at: <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/> (accessed August 25, 2020).
- Dean J (2005) Communicative capitalism: Circulation and the foreclosure of politics. *Cultural Politics* 1(1): 51–74.
- 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.
- Dienlin T and Metzger MJ (2016) An extended privacy Calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. Sample. *Journal of Computer-Mediated Communication* 21(5). Oxford Academic: 368–383.
- Doherty K, Balaskas A and Doherty G (2020) The design of ecological momentary assessment technologies. *Interacting with Computers* 32(3), 257–278. DOI: 10.1093/iwcomp/iwaa019
- Draper NA (2017) From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates: Challenging rational choice in digital privacy debates. *Policy & Internet* 9(2): 232–251.
- Draper NA and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.
- Epstein JM (1999) Agent-based computational models and generative social science. *Complexity* 4(5): 41–60.
- Esposti SD (2014) When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society* 12(2): 209–225.
- Festic N (2020) Same, same, but different! qualitative evidence on how algorithmic selection applications govern different life domains. *Regulation & Governance*. DOI: 10.1111/rego.12333.
- Frick NRJ, Wilms KL, Brachten F, et al. (2021) The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications* 47: 101046.
- Friedewald M (2018) Einleitung: Privatheit und selbstbestimmtes leben in der digitalenWelt. In: Friedewald M (ed.) *Privatheit und Selbstbestimmtes Leben in der Digitalen Welt: Interdisziplinäre Perspektiven auf Aktuelle Herausforderungen des Datenschutzes*. DuD-Fachbeiträge. Wiesbaden: Springer Fachmedien, pp. 1–10. DOI: 10.1007/978-3-658-21384-8_1
- Friedewald M, Wright D, Gutwirth S, et al. (2010) Privacy, data protection and emerging sciences and technologies: Towards a common framework. *Innovation: The European Journal of Social Science Research* 23(1): 61–67.
- Galluppi F, Lagorce X, Stromatias E, et al. (2015) A framework for plasticity implementation on the SpiNNaker neural architecture. *Frontiers in Neuroscience* 8, 1–20, Article 429. Frontiers. DOI: 10.3389/fnins.2014.00429
- Hamaker EL and Wichers M (2017) No time like the present: Discovering the hidden dynamics in intensive longitudinal data. *Current Directions in Psychological Science* 26(1). SAGE Publications Inc: 10–15.
- Hilbert M (2020) Digital technology and social change: The digital transformation of society from a historical perspective. *Dialogues in Clinical Neuroscience* 22(2): 189–194.
- Hildebrandt M (2008) Defining profiling: A New type of knowledge? In: Hildebrandt M and Gutwirth S (eds) *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Dordrecht: Springer Netherlands, pp. 17–45. DOI: 10.1007/978-1-4020-6914-7_2
- 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). 4.
- Jackson JC, Rand D, Lewis K, et al. (2017) Agent-Based modeling: A guide for social psychologists. *Social Psychological and Personality Science* 8(4): 387–395.
- Karapanos E (2020) Technology-assisted reconstruction: A new alternative to the experience sampling method. *Behaviour & Information Technology* 39(7). Taylor & Francis: 722–740.
- Kubey R, Larson R and Csikszentmihalyi M (1996) Experience sampling method applications to communication research questions. *Journal of Communication* 46(2). Oxford Academic: 99–120.
- Latzer M, Büchi M and Festic N (2019) Internet und Politik in der Schweiz 2019 [Internet and politics in Switzerland 2019]. Themenbericht aus dem World Internet Project—Switzerland 2019 [Report from the World Internet Project—Switzerland 2019]. Zurich: University of Zurich. DOI: 10.5167/uzh-176007
- Latzer M, Büchi M and Festic N (2020) Internet Use in Switzerland 2011–2019: Trends, Attitudes and Effects. Summary Report from the World Internet Project—Switzerland. Zurich: University of Zurich. DOI: 10.5167/uzh-186383

- Latzer M, Festic N and Kappeler K (2020) Coping Practices Related to Algorithmic Selection in Switzerland. The Significance of Algorithmic Selection for Everyday Life: The Case of Switzerland Report 4. Zurich, Switzerland: University of Zurich. DOI: 10.5167/uzh-190495
- Latzer M, Saurwein F and Just N (2019) Governance-Choice method: In search of the appropriate level of state intervention. In: Van den Bulck H (ed) *The Palgrave Handbook of Media Policy Research*. Basingstoke, UK: Palgrave Macmillan.
- Lempert R (2002) Agent-based modeling as organizational and public policy simulators. *Proceedings of the national academy of sciences* 99(suppl 3): 7195–7196. DOI: 10.1073/pnas.072079399
- Lupton D (2020) Thinking With care about personal data profiling: A more-than-human approach. *International Journal of Communication* 14: 3165–3183. Available at: <https://ijoc.org/index.php/ijoc/article/view/13540> (accessed June 2, 2020).
- Lyon D (2007) *Surveillance Studies: An Overview*. Polity.
- Lyon D (2014) Surveillance, Snowden, and Big data: Capacities, consequences, critique. *Big Data & Society* 1(2). SAGE Publications Ltd: 2053951714541861.
- Madsbjerg S (2017) It's time to Tax companies for using our personal data. The New York Times, 14 November. Available at: <https://www.nytimes.com/2017/11/14/business/dealbook/taxing-companies-for-using-our-personal-data.html> (accessed September 25, 2020).
- Mann M and Matzner T (2019) Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society* 6(2): 2053951719895805.
- Mann S and Ferenbok J (2013) New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society* 11(1/2): 18–34.
- Manokha I (2018) Surveillance, panopticism, and self-discipline in the digital Age. *Surveillance & Society* 16(2): 219–237.
- Marthews A and Tucker CE (2017) The impact of online surveillance on behavior. In: *Cambridge Handbook of Surveillance Law*. Cambridge, UK: Cambridge University Press, pp. 437–454. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3167473&download=yes (accessed June 4, 2020).
- Marx GT (2002) What's new about the 'New surveillance'? Classifying for change and continuity. *Surveillance & Society* 1(1): 9–29.
- Matzner T, Masur PK, Ochs C, et al. (2016) Do-It-Yourself data protection—empowerment or burden? In: Gutwirth S, Leenes R and De Hert P (eds) *Data protection on the move*. Dordrecht: Springer Netherlands, pp. 277–305. DOI: 10.1007/978-94-017-7376-8_11
- Morozov E (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs.
- Noble SU (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
- Ordoñez F (2020) Trump freezes green cards, many work visas until End of year. *NPR.org*, 20 June. Available at: <https://www.npr.org/2020/06/20/881245867/trump-expected-to-suspend-h-1b-other-visas-until-end-of-year> (accessed October 22, 2020).
- Penney JW (2016) Chilling effects: Online surveillance and wikipedia use. *Berkeley Technology Law Journal* 31(1): 117–182.
- Penney JW (2017) Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review* 6(2): 1–39.
- Preibusch S (2015) Privacy behaviors after Snowden. *Communications of the ACM* 58(5): 48–55.
- Richards NM (2013) The dangers of surveillance. *Harvard Law Review* 126(7): 1934–1965. Available at: https://www.jstor.org/stable/23415062?seq=1#metadata_info_tab_contents
- Richards NM and Hartzog W (2020) A Duty of Loyalty for Privacy Law. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217&download=yes
- Rosso M, Nasir A and Farhadloo M (2020) Chilling effects and the stock market response to the Snowden revelations. *New Media & Society* 22(11): 1976–1995.
- Schauer F (1978) Fear, risk and the first amendment: Unraveling the chilling effect. *Boston University Law Review* 58: 685–732.
- Schnauber-Stockmann A and Karnowski V (2020) Mobile devices as tools for Media and communication research: A scoping review on collecting self-report data in repeated measurement designs. *Communication Methods and Measures* 14(3), 145–164. Routledge. Available at: <https://www.tandfonline.com/doi/abs/10.1080/19312458.2020.1784402> (accessed August 11, 2020).
- Schneier B (2013) The public-private surveillance partnership. *Bloomberg.com*, 31 July. Available at: <https://www.bloomberg.com/opinion/articles/2013-07-31/the-public-private-surveillance-partnership> (accessed August 25, 2020).
- Schradie J (2019) *The Revolution That Wasn't: How Digital Activism Favors Conservatives*. Cambridge, MA; London, England: Harvard University Press.
- Schradie J (2020) The great equalizer reproduces inequality: How the digital divide Is a class power divide. In: Eidlín B and A. McCarthy M (eds) *Rethinking Class and Social Difference. Political Power and Social Theory*. Emerald Publishing Limited, pp. 81–101. DOI: 10.1108/S0198-871920200000037005
- Segijn CM and van Ooijen I (2020) Perceptions of techniques used to personalize messages across Media in real time. *Cyberpsychology, Behavior, and Social Networking* 23(5): 329–337.
- Segrin C (2014) Communication and personal well-being. In: Michalos AC (ed.) *Encyclopedia of Quality of Life and Well-Being Research*. Dordrecht: Springer Netherlands, pp. 1013–1017. DOI: 10.1007/978-94-007-0753-5_446
- Siles I, Segura-Castillo A, Solís R, et al. (2020) Folk theories of algorithmic recommendations on Spotify: Enacting data assemblages in the global south. *Big Data & Society* 7(1). SAGE Publications Ltd: 2053951720923377.
- Sklansky DA (2014) Too much information: How Not to think about privacy and the fourth amendment. *California Law Review* 102(5): 1069–1122. Available at: <https://heinonline.org/HOL/P?h=hein.journals/calr102&i=1113> (accessed August 6, 2020).
- Smith GJ (2018) Data doxa: The affective consequences of data practices. *Big Data & Society* 5(1). SAGE Publications Ltd: 2053951717751551.
- Solove DJ (2006) A taxonomy of privacy. *University of Pennsylvania Law Review* 154(3): 477–560.
- Solove DJ (2007) The first amendment as criminal procedure. *New York University Law Review* 82(1): 112–176. Available

- at: <https://heinonline.org/HOL/P?h=hein.journals/nylr82&i=124> (accessed July 21, 2020).
- Stoycheff E (2016) Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly* 93(2). Thousand Oaks: Sage Publications Inc: 296–311.
- Stoycheff E, Liu J, Xu K, et al. (2019) Privacy and the panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society* 21(3): 602–619.
- Suri RE (2004) A computational framework for cortical learning. *Biological Cybernetics* 90(6), 400–409. DOI: 10.1007/s00422-004-0487-1.
- Tanner A (2015) How Ads follow you from phone to desktop to tablet. *MIT Technology Review*, 1 July. Available at: <https://www.technologyreview.com/2015/07/01/167251/how-ads-follow-you-from-phone-to-desktop-to-tablet/> (accessed November 12, 2020).
- Taylor SE and Fiske ST (1978) Salience, attention, and attribution: Top of the head phenomena. In: *Advances in Experimental Social Psychology*. Elsevier, pp. 249–288. DOI: 10.1016/S0065-2601(08)60009-X
- Teknologirådet and Datatilsynet (2014) *Chilling Down in Norway*. Available at: https://www.datatilsynet.no/globalassets/global/english/nedkjoling-i-norge_eng_.pdf (accessed September 25, 2020).
- Trepte S (2021) The social Media privacy model: Privacy and communication in the light of social Media affordances. *Communication Theory* 31(4), 549–570. DOI: 10.1093/ct/qtz035.
- van Brakel R (2016) Pre-Emptive Big data surveillance and its (Dis)Empowering consequences: The case of predictive policing. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2772469.
- van Dijk J (2014) Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208.
- Van Dijk J (2020) *The Digital Divide*. Cambridge, UK: Polity.
- Véliz C (2020) *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. London, UK: Bantam Press.
- Vitak J and Zimmer M (2020) More than just privacy: Using contextual integrity to evaluate the long-term risks from COVID-19 surveillance technologies. *Social Media + Society* 6(3). SAGE Publications Ltd: 2056305120948250.
- Wachter S and Mittelstadt B (2019) A right to reasonable inferences: Re-thinking data protection Law in the Age of Big data and AI. *Columbia Business Law Review* 2019(2). 2: 494-620–494-620.
- White GL and Zimbaro PG (1975) *The Chilling Effects of Surveillance: Deindividuation and Reactance*. Ft. Belvoir: Defense Technical Information Center. Available at: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a013230.pdf>
- Wright D and Raab C (2014) Privacy principles, risks and harms. *International Review of Law, Computers & Technology* 28(3): 277–298.
- Ytre-Arne B and Das R (2021) Audiences' communicative agency in a datafied Age: Interpretative, relational and increasingly prospective. *Communication Theory* 31(4), 779–797. DOI: 10.1093/ct/qtaa018
- Ytre-Arne B and Moe H (2021) Folk theories of algorithms: Understanding digital irritation. *Media, Culture & Society*. 43(5), 807–824. Sage Publications Ltd: 0163443720972314. DOI: 10.1177/0163443720972314
- Zillmann D (2008) Excitation transfer theory. In: *The International Encyclopedia of Communication*. Wiley. DOI: 10.1002/9781405186407.wbiece049
- Zillmann D, Katcher AH and Milavsky B (1972) Excitation transfer from physical exercise to subsequent aggressive behavior. *Journal of Experimental Social Psychology* 8(3): 247–259.