

Triggers of a Sense of Dataveillance: Empirical Insights Into Characteristics and Determinants

Emerging Media

1–25

© The Author(s) 2025

Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/27523543251370597

journals.sagepub.com/home/emm



Céline Odermatt¹ , Noemi Festic¹ , Daniela Jaramillo-Dent¹ ,
Kiran Kappeler²  and Michael Latzer¹

Abstract

The automatic collection, storage, and analysis of user-generated digital traces by public and private actors (i.e., dataveillance) becomes salient to users through triggers of a sense of dataveillance. This can lead to a range of consequences, including democratically concerning responses such as the self-inhibition of legitimate digital communication behavior, known as the chilling effects of dataveillance. User-centered empirical research on the characteristics and determinants of such triggers remains scarce. Relying on a semistructured qualitative diary study with Swiss internet users, this article aims to map these triggers by (1) identifying and characterizing the triggers of a sense of dataveillance and (2) determining which everyday life events become triggers and why. The results show that triggers can be characterized by who initiates the everyday life event that becomes a trigger (i.e., corporate actors, public actors, private individual actors, and the self) and that everyday life events become triggers when users consume information about dataveillance or feel that they are or someone else is subjected to dataveillance. This is determined by the users' dataveillance imaginaries and the visibility of dataveillance practices. This article provides an innovative user-centered contribution to research on individual differences in experiencing triggers of a sense of dataveillance and hence adds to the empirical understanding of the formation of chilling effects.

Keywords

dataveillance, surveillance cues, perceived surveillance, chilling effects, diary study, qualitative

Received: April 14, 2025; revised: July 29, 2025; accepted: July 29, 2025

¹University of Zurich, Switzerland

²University of Copenhagen, Denmark

Corresponding Author:

Céline Odermatt, University of Zurich (IKMZ), Andreasstrasse 15, 8050 Zurich, Switzerland.

Email: c.odermatt@ikmz.uzh.ch



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons

Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use,

reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

Introduction

Individuals in digitalized societies generate a myriad of digital data traces when using digital services. This process makes many aspects of life more efficient and convenient for users, for instance through content personalization (Strycharz et al., 2019a), enhanced communication across platforms and apps, and innovative opportunities to participate in the digital economy (Plantin & Punathambekar, 2019). At the same time, public and private actors use such digital traces to monitor the online activities of users to gain economic profit and safeguard national security. This digital dataveillance entails the collection, retention, and analysis of digital traces in an automated, continuous, and unspecific manner (Büchi et al., 2022). The term differs from broader understandings of surveillance and emphasizes the impact of digital technology on personal or mass surveillance (Clarke, 1988). Dataveillance practices can become salient to individuals and elicit a feeling of being watched or listened to (Segijn & van Ooijen, 2020; Strycharz et al., 2022). Such a sense of dataveillance is subjective and does not require evidence of actual dataveillance. When individuals' sense of dataveillance is heightened, they can respond by self-inhibiting their legitimate communication behavior, a phenomenon known as the chilling effects of dataveillance (Büchi et al., 2022). Examples include people refraining from searching for information on sensitive topics, voicing their opinions, or disclosing personal information online. Such chilling effects are not desirable as they undermine the crucial role of digital communication in contemporary democratic societies: When digital communication is subjected to surveillance, people can be deterred from utilizing digital media for everyday activities, personal growth, societal participation, or political advocacy. From a societal perspective, limiting individuals' freedom to engage with digital media can have detrimental consequences (Büchi et al., 2022; Penney, 2022). Considering chilling effects as a potential danger of dataveillance, the question arises as to what elicits people's sense of dataveillance. We conceptualize events in everyday life that heighten people's sense of dataveillance, mediated by technology or not, as triggers of a sense of dataveillance. These triggers are the starting point of the causal mechanism of chilling effects and thus need to be investigated to understand the formation of a sense of dataveillance and subsequent behavioral modifications (Büchi et al., 2022). Due to the subjective nature of the sense of dataveillance, whether everyday life events become triggers varies at the individual level.

To deal with possible consequences of a sense of dataveillance and related societal risks, it is important to consider the governance of both dataveillance practices and their unintended and undesired consequences like chilling effects. Therefore, a thorough theoretical and empirical understanding of the formation of a sense of dataveillance and the factors contributing to individual differences in people's perceptions and responses is required. However, comprehensive and systematic user-centered empirical research on the formation of a sense of dataveillance remains scarce (Zhang et al., 2023). Thus, rather than investigating individual differences in perceptions of dataveillance and responses to a sense of dataveillance such as chilling effects (e.g., Kappeler et al., 2023), this study aims to map the specific triggers of a sense of dataveillance. It explores from a user perspective (1) what the triggers of a sense of dataveillance are and how they can be characterized, and (2) which everyday life events become triggers and why. To answer these research questions, we conducted an in situ qualitative digital diary study with internet users in Switzerland. First, the results include a systematic characterization of online and offline triggers of a sense of dataveillance based on the perceived trigger-initiating actors. Second, our findings show that everyday life events become triggers when users consume information about dataveillance or when they feel that they are or someone else is subjected to dataveillance. Determinants of such events becoming triggers are users' dataveillance imaginaries (Kappeler et al., 2023) at

the person level and the visibility of dataveillance practices at the trigger level. We also found that triggers can activate negative feelings in users when they consider the intrusiveness of dataveillance disproportionate to its purpose, they are uncertain about how dataveillance works, and user agency is low. Hence, this study expands on prior theoretical research on the causal mechanism of chilling effects (Büchi et al., 2022) and adds to user-centered empirical research on the sense of dataveillance (Strycharz et al., 2022; Zhang et al., 2023) by examining how triggers form such a sense of dataveillance and by exploring the subjective nature of triggers as well as the possible consequences of an increased sense of dataveillance.

Theoretical Background

Defining Dataveillance

Contemporary dataveillance practices have been facilitated by the advent of digitalization. Their societal relevance can be understood in the context of three characterizing coevolutionary socio-technical transformations: datafication, algorithmization, and platformization, also known as the digital trinity (Latzer, 2022). In a nutshell, datafication reproduces various aspects of life in the form of (big) data, algorithmization extracts capital from these data, and the platformization of diverse markets optimizes the organizational conditions for further datafication and algorithmization (Latzer, 2022).

These three processes have also affected surveillance practices. While traditional understandings of surveillance before digitalization concerned individuals and physical spaces, the subjects of current dataveillance practices are disembodied and deterritorialized data points representing individuals or spaces. Due to the unprecedented amount of data points generated in digitized societies, dataveillance practices have exposed new areas of life to surveillance and allowed for the combined analysis of linked data points, expanding the overall impact of traditional surveillance (Clarke, 2019). Thus, dataveillance has become an infrastructural practice combining data from formerly distinct spheres (Lyon, 2022) and accumulating them into an ecosystem of connective media (van Dijck, 2014).

Dataveillance is therefore defined as the collection, retention, and analysis of digital traces in automated, continuous, and often unspecific ways (Büchi et al., 2022; Lyon, 2022; van Dijck, 2014). It aims at capitalizing on its outcomes using algorithmic selection (e.g., through the personalization of content). This has implications for privacy, and such profiling can, for instance, lead to the discrimination of certain groups and individuals (Büchi et al., 2020; Clarke, 2019).

The Chilling Effects of Dataveillance

At the individual level, a heightened sense of dataveillance can lead to behavioral responses such as the self-inhibition of legitimate digital communication behavior, a phenomenon referred to as the chilling effects of dataveillance (Büchi et al., 2022; Penney, 2022; Solove, 2006; Stoycheff, 2016, 2023). The causal process of chilling effects was theoretically modeled by Büchi et al. (2022; Figure 1).

According to this model, a sense of dataveillance can be heightened through salience shocks, which include triggers of a sense of dataveillance. This increases people's expectations of negative outcomes resulting from engaging in uninhibited digital communication behaviors, renders their attitudes toward them less favorable, and lowers their intention to engage in them, which leads people to inhibit themselves online (Büchi et al., 2022).

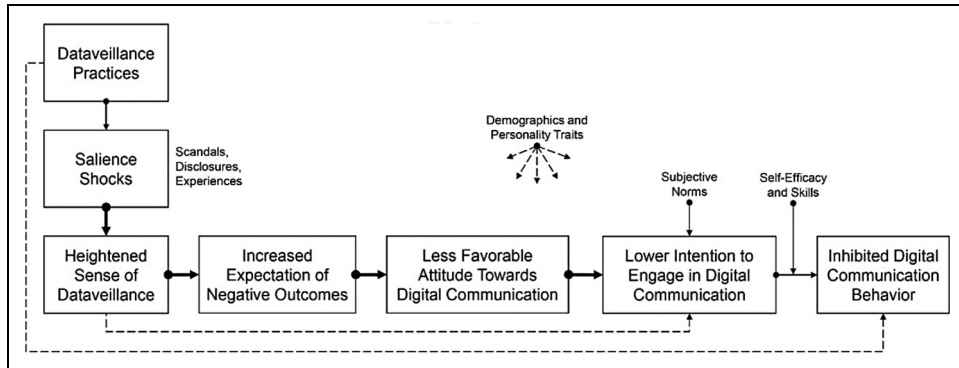


Figure 1. Mechanisms of the Chilling Effect of Dataveillance Practices on Digital Communication.

Note. From “The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda,” by M. Büchi, N. Festic, and M. Latzer, 2022, *Big Data & Society*, 9(1), p. 7 (<https://doi.org/10.1177/20539517211065368>).

This model provides the theoretical context for this study and emphasizes the relevance of the concept of a sense of dataveillance as the starting point for the chilling effects hypothesis—an undesirable phenomenon that has been empirically evidenced: A representative online survey in Switzerland found that around 80% of the online population reported self-inhibition in information search, opinion expression, or information disclosure online (Latzer et al., 2023b). Empirical research has explored how users imagine dataveillance and how this connects to self-inhibition online (Kappeler et al., 2023). Yet, this high prevalence of self-reported chilling effects highlights the need for more in-depth investigations into how a sense of dataveillance is formed.

The Formation of a Sense of Dataveillance

A sense of dataveillance is the cause of the self-inhibition of digital communication behaviors (Büchi et al., 2022). This feeling of being watched or listened to online has also been discussed under the term perceived surveillance (Strycharz & Segijn, 2022) and has been linked to other user responses, such as enhanced privacy protection measures (Strycharz & Segijn, 2024). This study focuses on the concept of dataveillance as opposed to the broader concept of surveillance to emphasize the role of digital technology (Kappeler et al., 2023). In addition, we use the term sense rather than perception to reflect the experiential dimension of the concept.

Experiencing a sense of dataveillance is inherently subjective because it does not require evidence of being subjected to dataveillance. Rather, individuals’ degree of confidence in being subjected to dataveillance can vary. Thus, the sense of dataveillance resembles a belief-like state not necessarily constrained by the truth (Arcangeli, 2019; Kind, 2016). This relates to the psychological notion of thought confidence (i.e., the general state of certainty in one’s thoughts; Tormala et al., 2008). This thought confidence can affect the perception of information, shape the responses to it (Grigorios et al., 2022), and affect subjective knowledge formation (Kruglanski, 1990). Empirical research indicates that thought confidence affects the perceived validity of and reliance on cognitive responses (Petty et al., 2002) and is influenced by individuals’ emotions that become salient when exposed to information (Petty & Briñol, 2014; Stavraki et al., 2021). Applying the notion of thought confidence to a sense of dataveillance and the triggers that lead to it, individuals’

confidence in being subjected to dataveillance can arguably vary. This, in turn, can affect whether everyday life events become triggers and how dataveillance imaginaries are formed.

The Triggers of a Sense of Dataveillance. Individuals' sense of dataveillance increases when dataveillance becomes salient to them (Büchi et al., 2022). Everyday life events that make dataveillance salient and thereby elicit or heighten individuals' sense of dataveillance can be defined as triggers of a sense of dataveillance. Within the theoretical model of the chilling effects of dataveillance (Büchi et al., 2022), these triggers are considered a subgroup of salience shocks (see Figure 1) because they entail subtle and habitual events in everyday life and do not focus on disruptive shocks such as public disclosures and scandals.

This understanding of triggers is rooted in discussions on cues of traditional surveillance of individuals and physical spaces (White & Zimbardo, 1975) and the watching eyes effect (Penney, 2022): Empirical research in psychology and behavioral economics has demonstrated that images of eyes glancing at individuals can create a sense of being watched, which, in turn, increases norm-conforming behavior and reduces antisocial behavior (Dear et al., 2019; Manesi et al., 2016). Such behavioral responses have also been found for surveillance cues like closed-circuit television (CCTV) cameras (Jansen et al., 2018), body cameras (Ariel et al., 2018), and eye-tracking technology (Nasiopoulos et al., 2015).

Translating these findings to digital societies, a comprehensive understanding of what triggers a sense of dataveillance is missing. A fragmented body of research has suggested a list of everyday life events that are likely to heighten a sense of dataveillance in internet users. These include dataveillance-related news articles (Penney, 2016), personalized advertisements (Frick et al., 2021; Grigorios et al., 2022; Strycharz et al., 2019a; Strycharz & Segijn, 2022), notifications about data regulations (Shankar et al., 2021; Stoycheff, 2016), disclosure of (sensitive) information (Dev et al., 2020; van Schaik et al., 2018), self-monitoring practices (Lupton & Michael, 2017), other people's information sharing behaviors (Spottswood, 2017), and being contacted by strangers (Dev et al., 2020).

Furthermore, Zhang et al. (2023) found that technologies and devices (e.g., apps, smartphones, speakers, watches, and web browsers) can trigger a sense of dataveillance in users, but it is unclear which aspects of these technologies do this. In line with Neisser (1978), whether an everyday life event becomes a trigger is determined by people's dataveillance imaginaries (their schemata), the characteristics of the event (the available information), and how the event is experienced (exploration). In turn, the perception of everyday life events as triggers shapes dataveillance imaginaries and the anticipation of future triggers.

While previous studies have analyzed attitudes and reactions of users to specific triggers of a sense of dataveillance using quantitative surveys (e.g., Frick et al., 2021; Zhang et al., 2023), experimental designs (e.g., Stoycheff, 2016), web traffic analysis (Penney, 2016; Penney et al., 2025), and qualitative focus groups (Lupton & Michael, 2017), these designs employed predefined triggers of a sense of dataveillance and did not gather an extensive list of triggers due to not allowing for open answers or having a different focus. Hence, there is a lack of user-centered, comprehensive, and systematic research on what the triggers of a sense of dataveillance are and how they are characterized, which is needed to thoroughly understand the formation of a sense of dataveillance (Büchi et al., 2022).

Dataveillance Imaginaries. A sense of dataveillance is not only elicited by triggers but also further shaped by individuals' dataveillance imaginaries (Kappeler et al., 2023). Such sense-making processes of digital technologies by internet users have been explored in prior research under various

terms. In digital advertising research, the concept of surveillance beliefs pertaining to ideas about the extent and purpose of surveillance has been linked to the extent of perceived surveillance. Surveillance beliefs are shaped by information about surveillance practices and by people's past experiences with digital technology (Strycharz & Segijn, 2022). Personal understandings of dataveillance are also discussed in the context of folk theories, which individuals rely on to comprehend phenomena in everyday life, such as technological systems (DeVito et al., 2017; Zhang et al., 2024), algorithms in the media (Ytre-Arne & Moe, 2021), or algorithmic profiling (Büchi et al., 2023). Recently, people's sense-making processes of dataveillance have also been put into context with the notion of imaginaries, offering a more socially grounded and comprehensive perspective (Kappeler et al., 2023). Rather than focusing only on personal understandings of context- or device-specific surveillance (Segijn et al., 2025; Strycharz & Segijn, 2022) or on subjective assumptions about how systems and algorithms work (DeVito et al., 2017; Siles et al., 2020), imaginaries are understood to be shaped by both individual experiences and broader demographic and sociocultural contexts (Bucher, 2017). Thus, they reflect both personal sense making and the social structures in which it unfolds. Imaginaries encompass entire data ecosystems and help explain broader behavioral responses, such as self-inhibition, beyond specific contexts or technologies (Kappeler et al., 2023).

Empirical research indicates that dataveillance imaginaries differ in terms of the actors, workings, data types, and consequences of dataveillance (Kappeler et al., 2023). Furthermore, Zhang et al. (2023) found that users imagine diverse purposes of dataveillance practices ranging from advertising and personalization to research and the manipulation of opinions and behaviors.

While such imaginaries are not necessarily based on factual information or expert views, they impact individuals' sense of dataveillance and their responses to it (Kappeler et al., 2023). Therefore, while dataveillance imaginaries can be shaped by experiencing triggers of a sense of dataveillance, they can also affect whether an everyday life event becomes a trigger, implying that an event that triggers one person's sense of dataveillance might not do so for another. While empirical research on dataveillance imaginaries is emerging (Kappeler et al., 2023), the factors determining whether everyday life events become triggers of a sense of dataveillance are underexplored. It also remains unclear how the interplay between characteristics of an event, people's dataveillance imaginaries, and their anticipation of triggers might relate to experiencing events as triggers.

Method

To explore this study's research objective (i.e., mapping the triggers of a sense of dataveillance), a semi-structured, solicited, and event-based digital diary study was conducted with Swiss internet users. This method ensures in situ reporting of events and minimizes recall bias in participants (Bartlett & Milligan, 2015), which has been a limitation of data collection methods employed thus far to explore events triggering a sense of dataveillance (e.g., Bucher, 2017).

Recruitment and Sample

We recruited participants through an advertisement posted on public marketplace websites of various Swiss universities and disseminated it to the extended network of the research team. The study was framed as an opportunity to actively contribute to academic research to recruit people interested in the topic and motivated to contribute to research. For this purpose, the study instructions disclosed the research goals, and the inclusion criteria for participants were: 18 years of age or older,

internet users, and interested in internet-related topics, which we chose to heighten the participants' awareness of the topic to ensure comprehensive reporting of triggers. First, participants received a short screening questionnaire about their daily amount of internet use, self-reported internet skills, and sociodemographic characteristics. Then, aiming for variation in the sample, participants were individually contacted based on age, gender, education level, and internet skills and asked to sign up for participation and provide written informed consent. Table 1 displays the final sample. All participant information is anonymized. After the study, participants received a small remuneration.

Data Collection

Between July and October 2022, we asked the participants to report on WhatsApp or Signal at least daily for 4 weeks about triggers of a sense of dataveillance they experienced. Because the recruitment was rolling, participants started at various times but participated for the same duration each. We prompted participants at the beginning of their participation to report whether they experienced an event where they felt that their data were collected and analyzed, felt monitored, encountered the dataveillance topic in another way, or thought another person might think of the topic. In such a case, we asked participants to describe the situation and provide contextual details about their activities at the time, the people involved, and if they were using a device or service. The study instructions summarized this information and were always accessible to participants. Participants then sent us their reports once per day on their own schedule. When they did not send a message for more than two consecutive days, we sent a reminder message asking for a report in hindsight. All materials of the recruitment and data collection are shared on Figshare.¹

Description of Data

In total, the data set comprises $N=276$ triggers of a sense of dataveillance. The reports consisted of multimodal data including text or voice messages and screenshots, pictures, or links providing more

Table 1. Sample Characteristics.

Pseudonym	Gender	Age	Education	Internet Use Time (h Per Day)	Internet Skills
Denis	M	27	High	4.5	Good
Maria	F	26	High	4	Excellent
Anna	F	27	High	10	Excellent
Robert	M	34	Medium	4	Very good
Monika	F	56	High	5	Sufficient
Elena	F	35	High	16	Very good
Jose	M	41	High	12	Very good
Tatjana	F	29	Medium	8	Very good
Natalia	F	21	Medium	4	Good
Katharina	F	30	High	10	Excellent
Daniel	M	26	High	8	Excellent
Irina	F	32	High	11	Excellent
Daria	F	21	High	6	Very good
Vera	F	24	High	8	Very good
Ivan	M	32	High	5	Very good
Laura	F	23	High	6	Very good
Paul	M	40	Low	3	Very good

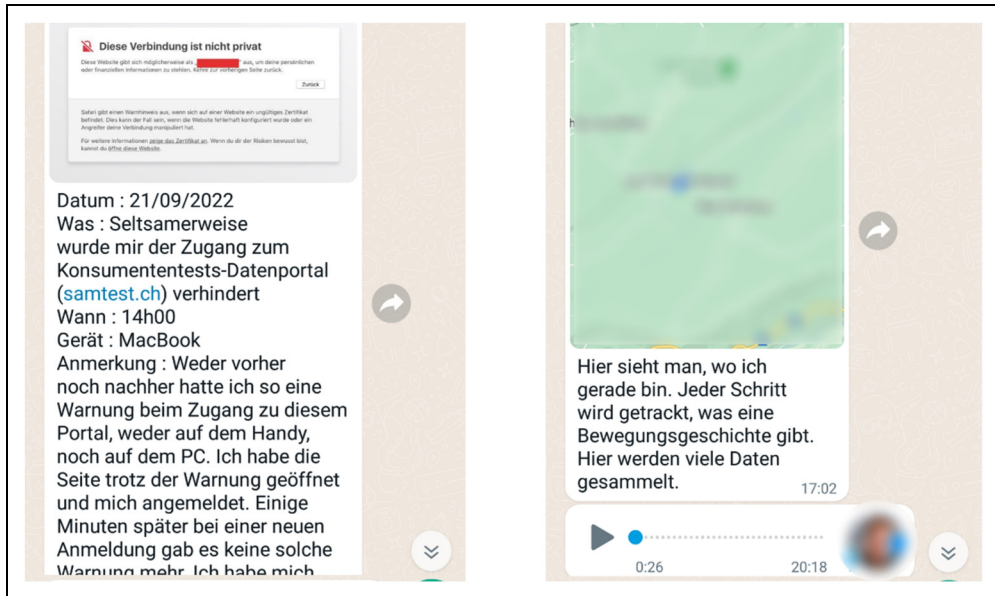


Figure 2. Examples of Reports with Multimodal Data.

detailed information about the trigger as shown in Figure 2. The between-person differences in frequency of reports of triggers were high, with some participants reporting them multiple times a day and others only a few times a week. Participants often provided additional information about their experiences, including assessments, opinions, and explanations of triggers, the life domains in which they occurred, the people involved, and the devices, services, or applications used.

Data Analysis

The reports were transcribed (Meredith, 2016) and analyzed using qualitative content analysis, which offers a systematic approach to categorize and interpret multimodal qualitative data (Puppis, 2019). First, broad categories of triggers of a sense of dataveillance were deductively derived from the literature (Penney, 2016; Stoycheff, 2016; Strycharz et al., 2022). These included news reports, digital notifications about data policy, and personalized ads or feeds. Because participants were asked to not only report triggers that they experienced when using the internet but also in all domains of everyday life, triggers were expected to occur both online and offline. The derived examples of triggers and their mode (online/offline) built an initial deductive coding framework. Through inductive open coding, additional themes emerged from the data which reflected categories of triggers expanding the initial framework. The unit of analysis comprised single events reported by participants, which triggered their sense of dataveillance. Additional information about the triggers as well as the participants' use of language in describing them were also coded and categorized. The first round of coding was conducted with the reports in their original language (i.e., German) by the main coder, a native speaker. To enable collaboration in the research team during the coding process, the coded sequences were translated into English. The main coder, also fluent in English, regularly referred to the original reports throughout the coding process to avoid losing critical information due to translation. To further ensure semantic accuracy, the research team

collaboratively discussed idiomatic expressions and ambiguous phrases and documented implied meanings and emotional tone through analytic memos (Vanover et al., 2022). Finally, the main coder cross-checked key quotes against the original entries.

Findings

This section discusses our findings. First, we present a characterization of online and offline triggers of a sense of dataveillance based on the perceived trigger-initiating actors (i.e., corporate actors, public actors, private individual actors, and the self). Second, we explore the everyday life events that became triggers, and their determinants. Triggers occurred when users consumed information about dataveillance or felt that they were or someone else was subjected to it. For all triggers, at the person level, dataveillance imaginaries were an important determinant in everyday life events becoming triggers. Additionally, when users felt subjected to dataveillance, at the trigger level, the visibility of dataveillance practices determined whether an everyday life event became a trigger.

We also found that triggers activated negative feelings when the perceived intrusiveness of dataveillance was disproportionate to its purpose, when users were uncertain about how dataveillance works, and when user agency was low.

Characterization of the Triggers of a Sense of Dataveillance

The reports of triggers of a sense of dataveillance in our sample confirmed that triggers occurred both online and offline (i.e., when participants actively used the internet or digital technology and when they did not). When describing the triggers, the participants identified the perceived actors who initiated the events that became triggers. They considered these actors responsible for the occurrence of the trigger. Participants identified these actors from the available information about the trigger and their own dataveillance imaginaries. This revealed that triggers included events that not only happened to participants due to other actors but also events initiated by participants themselves. Based on the reported trigger-initiating actors, a characterization of online and offline triggers of a sense of dataveillance was created (Table 2).

In many instances, the same type of trigger was experienced both online and offline, such as self-initiated information-seeking practices. Although all types of triggers could theoretically occur online and offline, some were only reported in one mode. For example, privacy breaches initiated by corporate actors were only reported offline. Although possible, similar online events such as data leaks by social media platforms were not mentioned by participants. Corporate actors and participants themselves were the most named trigger-initiating actors, followed by other individuals and public actors.

Everyday Life Events as Triggers of a Sense of Dataveillance

Everyday life events became triggers of a sense of dataveillance when participants consumed information about dataveillance or when they felt that they were or someone else was subjected to it. Feeling subjected to dataveillance was either immediate or anticipated: participants either felt subjected at the time of the trigger or anticipated being subjected at a later point, indicating a temporal dimension in perceiving dataveillance.

The distinction between consuming dataveillance-related information and feeling subjected to dataveillance is in line with literature suggesting that a sense of dataveillance can be influenced by both public scandals about dataveillance practices and personal experiences (Büchi et al., 2022).

Table 2. Characterization of Triggers of a Sense of Dataveillance.

Trigger-Initiating Actor (Who Initiated the Everyday Life Event that Triggered a Sense of Dataveillance?)	Trigger Mode (In What Mode did the Everyday Life Event that Triggered a Sense of Dataveillance Occur?)	
	Online	Offline
Corporate actors (e.g., private companies, organizations, stores, platforms, device manufacturers)	<p>Notifications: seeing notifications for changes of data policies of platforms and services, cookies, privacy warnings by browsers and tracking blockers, current mobile data use from mobile phone provider, updates on financial transactions, data collection cues on smartphones (e.g., visual indications that microphone/camera are activated)</p> <p>Customer retention measures: seeing personalized content (e.g., ads, feeds, commercial offers, automatically generated emojis, and spam) and ads containing dataveillance-related information</p> <p>Service access requirements: facing a requirement to disclose personal information to use a service (e.g., online forms to access a free trial, to create a profile, to use a job application tool, or to perform commercial transactions)</p>	<p>Customer retention measures: seeing physical ads in public spaces containing dataveillance-related information (e.g., statistics of customer data of an online shop)</p> <p>Service access requirements: being required to use an access control device (e.g., scanning a membership bracelet to enter the gym)</p> <p>Public postings: seeing a QR code on a sticker on a railing</p> <p>Privacy breaches: having access to other customers' private information without authorization (e.g., receiving another person's phone bill)</p>
Public actors (e.g., public administrations, governmental actors, public institutions)	<p>Service access requirements: facing a requirement to agree with a data protection declaration to use a service (e.g., to submit a job application)</p>	<p>Public postings: seeing notices of citizen surveillance through CCTV and Wi-Fi data collection at a metro station, seeing a QR code (e.g., on a sign in a public library)</p>

(continued)

Table 2. Continued.

Trigger-Initiating Actor (Who Initiated the Everyday Life Event that Triggered a Sense of Dataveillance?)	Trigger Mode (In What Mode did the Everyday Life Event that Triggered a Sense of Dataveillance Occur?)	
	Online	Offline
Private individual actors (e.g., other (un)known individuals)	Privacy breaches: experiencing hacking and phishing attempts by strangers (e.g., hacking attack on devices, requests by fake profiles on social media)	Privacy breaches: having access to other customers' private information without authorization (e.g., a train conductor digitally registering and loudly reading out personal information of a passenger without a ticket) Privacy notices: receiving a data protection reminder from an employer
	Observation of privacy measures: other people avoiding certain digital services (e.g., WhatsApp) or disclosing personal information online	Observation of privacy measures: other people formally refusing consent to photographs (e.g., not signing a permission slip), withholding or anonymizing personal information when asked by others, and avoiding credit card payments
Self (i.e., participants)	Information-seeking practices: seeking information about dataveillance-related topics in news articles, blogs, podcasts, and radio shows	Information-seeking practices: seeking information about dataveillance-related topics in offline news articles or museums
	Self-expression practices: participating on social media (e.g., updating a profile or posting content), in opinion surveys (e.g., market or customer experience research), and in digitally mediated conversations about dataveillance-related topics (e.g., on a messenger service, phone, or video call)	Self-expression practices: participating in in-person conversations about dataveillance-related topics
	Self-monitoring practices: allowing the status and history of own online activities, tracking own location with a smartphone or wristband, synchronizing a service on multiple devices (e.g., WhatsApp on desktop and smartphone)	Self-monitoring practices: undergoing medical examinations (e.g., blood donation and general health check-up)

(continued)

Table 2. Continued.

Trigger-Initiating Actor (Who Initiated the Everyday Life Event that Triggered a Sense of Dataveillance?)	Trigger Mode (In What Mode did the Everyday Life Event that Triggered a Sense of Dataveillance Occur?)	
	Online	Offline
	Personal privacy measures: avoiding certain services and devices (e.g., work laptop), using a browser in private mode, using ad and tracking blockers	

This finding further mirrors the distinction between information- and experience-driven surveillance beliefs in the dataveillance effects in advertising landscape framework (Strycharz & Segijn, 2022).

Consuming Information About Dataveillance. In some cases, the participants’ sense of dataveillance was triggered by consuming information about dataveillance as a general concept or idea. Because the information consumed was not about the participants’ own behaviors, they did not feel subjected to dataveillance when these triggers occurred. For instance, Daniel (m, 26) read news articles about Google Chrome’s dataveillance practices:

Google Chrome (...) scans the operating system and all data on the computer to check if these could conflict with Chrome addons. In other words, Alphabet is spying on user data under this pretense without anyone having ever consented to it and without informing users – maybe [they did] in the terms of service. I wonder if this is even legal.

This event triggered Daniel’s sense of dataveillance because he consumed explicit information about dataveillance practices. Considering that the consumption of information can heighten the anticipation of similar future information (Neisser, 1978), it is likely that other everyday life events related to Google or similar corporate actors, which may not have triggered Daniel’s sense of dataveillance before, will do so in the future. As these news articles were addressed to a larger audience and were not directly tied to his online search behavior, Daniel did not express a feeling of being subjected to dataveillance when experiencing the trigger.

Feeling Subjected to Dataveillance. In other cases, participants experienced triggers within everyday life events where they felt that they were or someone else was subjected to dataveillance.

Feeling Themselves Subjected to Dataveillance. Most triggers in our sample were reported as personal experiences of being subjected to dataveillance. For example, Katharina (f, 30) felt subjected to dataveillance when she had to disclose sociodemographic information to order from an online retailer:

You are asked for your exact date of birth on the grounds of the protection of minors. It would be less intrusive (and therefore more proportionate) if you simply had to confirm with “yes” or “no” whether you are already 18 years old. In this case, personal data are unnecessarily collected.

Because Katharina was required to disclose her own information, she felt subjected to dataveillance. She further considered the retailer responsible for initiating this trigger when describing the required information disclosure. This reflects experience-driven surveillance beliefs discussed in advertising studies, where consumers become aware of targeting practices through experiences rather than explicit information (Strycharz & Segijn, 2022).

These examples from Daniel and Katharina further show that participants can have negative feelings toward triggers of a sense of dataveillance when they consider dataveillance disproportionate to its perceived purpose. Daniel considered Google Chrome’s dataveillance practices a violation of user rights because of a lack of conscious consent. His emphasis on reading about this in the news implies his initial unawareness of it. He considered the company’s practices highly questionable, using accusatory terms like “spying” and questioning their legality. Daniel thus demanded information transparency from the company about its dataveillance practices. His mentioned lack of knowledge about the terms of service and users’ consent to such extensive dataveillance relates to debates about online consent processes (Solove, 2013). Studies have shown that users tend to perceive terms of service policies as a nuisance and habitually agree to them without reading them (Obar & Oeldorf-Hirsch, 2020).

Similarly, Katharina deemed the dataveillance practices violating and disproportionate to their perceived purpose, as reflected in her description of the event as intrusive and unnecessary, despite the clearly communicated purpose of dataveillance. This contradicts research suggesting that overt data collection promotes favorable affective responses in consumers (Aguirre et al., 2015; Grigorios et al., 2022; Segijn et al., 2021). Instead, Katharina’s example implied that transparent data collection alone is not sufficient for favorable user attitudes toward perceived dataveillance practices, but the degree of intrusiveness of dataveillance needs to be proportionate to its communicated purpose. Empirical research has shown that trust in institutions and low levels of anxiety among consumers are central to positive attitudes toward disclosing personal data (Robinson, 2018), which were both lacking in Katharina’s case. By her placing the order despite privacy concerns, the example alludes to privacy calculus research suggesting that whether users disclose personal information to use a service or purchase a product depends on their rational assessment of perceived privacy concerns and benefits of information disclosure (Plangger & Montecchi, 2020).

Everyday life events also became triggers when participants anticipated being subjected to dataveillance. Jose (m, 41) reported such an experience when seeing a Quick Response (QR) code on a walk (Figure 3).

Jose commented:

I was not sure if I should scan the QR code because there was no information about it at all and I thought I might be directed to an unsafe website.

Jose did not scan the QR code due to data security concerns, which outweighed his curiosity about it. While he was therefore not subjected to dataveillance when experiencing the trigger, he anticipated that scanning the code would subject him to it. The lack of additional information left Jose somewhat uncertain about the workings of dataveillance and whether his anticipation of data security threats was justified, which he expressed with caution and suspicion toward the trigger.



Figure 3. Picture of the QR Code Sent by Jose.
QR: Quick Response.

Feeling That Someone Else is Subjected to Dataveillance. Besides consuming information about dataveillance and feeling themselves subjected to it, some participants' sense of dataveillance was triggered when they felt that other people were subjected to dataveillance. For example, Natalia (f, 21) watched a presentation on Zoom about a study program in sexual education and felt that other people in the video call were subjected to dataveillance:

The presenters are talking quite openly (...) about their topics and the study program. (...) Many of them have their cameras turned on. I think it's very interesting how very different it can be [for each person] how much they want to reveal of themselves (...) and that for some people it doesn't matter what they reveal of themselves and where.

Although Natalia participated in the same video call as the presenters, the presenters' online communication behavior rather than her own triggered her sense of dataveillance. The presenters openly talked about sexuality, a topic that Natalia seemed to perceive as rather sensitive, and they revealed their faces while presenting. She pointed out the subjective differences in views on privacy protection and claimed that "some people" (i.e., the presenters) are rather careless about their privacy. By emphasizing the behavior of "some people", Natalia implied that she would be more cautious about her own privacy. This experience led Natalia to feel that the presenters were, but she herself was not subjected to dataveillance.

Determinants of Everyday Life Events Becoming Triggers of a Sense of Dataveillance. The everyday life events reported as triggers varied between the participants. Some triggers (e.g., personalized ads and cookie notifications) were reported by most participants, which reflects commonly discussed

online triggers in extant literature (Shankar et al., 2021; Stoycheff, 2023; Strycharz et al., 2019a; Strycharz & Segijn, 2022). Still, a few participants never reported common triggers such as cookie notifications, which is notable considering the legal requirement for cookie consent under the General Data Protection Regulation (GDPR) (Hu & Sastry, 2019) and given that all participants in our sample were internet users and likely encountered some form of cookie notification. Furthermore, some triggers, such as personal privacy measures and service access requirements, were reported by only a few participants in our sample despite the plausibility that they were experienced by most participants. Hence, we argue that whether an everyday life event became a trigger of a sense of dataveillance was personal and subjective.

Our data revealed two determinants for whether an everyday life event became a trigger: (1) personal dataveillance imaginaries and (2) the trigger-related visibility of dataveillance practices. Dataveillance imaginaries were an important person-level determinant for all triggers, whereas the visibility of dataveillance practices was an important trigger-level determinant for the instances in which the participants felt subjected to dataveillance.

Users' Dataveillance Imaginaries. All everyday life events that became triggers in our sample were determined by the participants' dataveillance imaginaries (i.e., who they think does what to what data and with what consequences; Kappeler et al., 2023). Participants expressed their imaginaries either explicitly in their reports or through interpretive narratives.

Returning to the example of Daniel consuming information about Google Chrome's dataveillance practices through news articles, his dataveillance imaginaries played a role in determining that this everyday life event triggered his sense of dataveillance and in his interpretation of it. His use of the word "spying" and his questioning of the practices' legality implied that Daniel imagined corporate actors engaging in deceitful dataveillance practices that exploit users' tendency not to (carefully) read terms of service (Obar & Oeldorf-Hirsch, 2020). He also imagined that users would not consent if explicitly asked. Hence, the article became a trigger because consuming the information activated Daniel's cognitive processes and led him to connect the event to his imaginaries about dataveillance workings and the corporate actors involved.

Dataveillance imaginaries also determined whether everyday life events where participants felt that they were or someone else was subjected to dataveillance became triggers. In many cases, such triggers were an assumed result of dataveillance, such as personalized ads. Laura (f, 23), for instance, saw an Instagram ad for a student discount (Figure 4).

Laura reported:

They know I'm a university student.

Laura sensed that the ad was a result of dataveillance although it was not clearly communicated to her. She remarked that "they", that is, the platform and advertiser, "know" her current education status and have thus initiated this trigger. This implied she felt subjected to dataveillance even without clear information about actual dataveillance practices. Hence, Laura engaged in sense-making processes relying on her dataveillance imaginaries, which informed her about the kind of collected and analyzed data, the actors involved, and the personalization process.

Furthermore, referring to the platform, algorithmic processes, and the advertiser as "they" speaks to the personification of surveillance, a common theme in folk theories (Siles et al., 2019, 2020) arising from personal experiences with algorithmic workings rather than factual information about dataveillance (Dogruel, 2021). Empirical research has shown that algorithms and algorithmic-



Figure 4. Screenshot of the Ad Sent by Laura.

selection applications are often imagined as human-like entities (Festic, 2022; Siles et al., 2020) conveying the meaning that “someone is watching you” (Kelly, 2022, p. 173).

Similarly, Robert (m, 34) felt subjected to dataveillance when he saw a personalized news feed with heart-shaped buttons to “like” articles he was interested in:

Here I can like Google [News] articles, which generates data collection and the favoring of [certain] articles.

This example reflects a few elements of Robert’s dataveillance imaginaries. First, although Robert did not see explicit information on the platform about the effects of “liking” content, he had a clear idea of his role in steering dataveillance practices. He emphasized feeling subjected to dataveillance by stating that this action “generates data collection”. Second, the connection Robert makes between the interactive functionalities of the platform (“like” button) and the expected outcome of his interaction (favoring articles) was thus rooted in his dataveillance imaginaries. These imaginaries will likely be reinforced if future news suggestions align with the intentionally liked content, and Robert likely anticipates personalized content in the future.

Such personalized content activated negative feelings in Laura, but positive feelings in Robert, depending on the perceived degree of user agency. Laura sensed the personalized ad on Instagram as an intrusion, evoking powerlessness and unease. This aligns with studies showing that covert

dataveillance practices promote unfavorable user attitudes (Grigorios et al., 2022). Specifically for personalized advertisements, rejection and privacy concerns are more likely when users are not informed about data collection (Boerman et al., 2021; Strycharz et al., 2019b). Like Laura, users then tend to feel vulnerable and uncomfortable (Aguirre et al., 2015; Herder & Zhang, 2019). The ad's unexpectedness, combined with Laura's imaginaries about personal data collection, left her feeling without agency as the event could neither be undone nor changed.

Robert's example shows that when users perceive high agency, personalized content can activate positive feelings. His intention to curate his news feed speaks to research on users' perceived capabilities to steer and alter outcomes of dataveillance practices in digital media. Such microlevel algorithm engagement reflects low-effort, routine productive acts aimed at strategically steering one's media experience (Kapsch, 2022).

By pointing out his capability to act ("I *can like* articles"), Robert highlights his agency facilitated by the functionality of the platform (i.e., the "like" button) and positively describes the expected outcome of data analysis ("favoring"). Unlike Laura, he implied no concerns regarding data collection. He instead had a favorable attitude toward personalized content and acted to improve such recommendations.

Everyday life events also became triggers because some participants noticed implicit dataveillance cues, which they explained based on their dataveillance imaginaries. For example, Natalia saw a dot on her smartphone screen and understood it as a cue for background data collection by an app:

When I have WhatsApp running in the background on my iPhone, a green or orange dot appears in the upper right corner. I assume that the microphone or the camera are still running in these moments even though I don't consciously want this.

Seeing the dot activated her sense-making processes, exemplified by her statement associating it with technical features on the device and a specific app despite no clear evidence for it. This reflects her dataveillance imaginaries about the workings and actors of dataveillance, according to which apps can employ technical features of a device for dataveillance purposes without obtaining users' consent. Yet, by saying she "assumes" that this is the case, she expressed an uncertainty about such dataveillance workings. She emphasized that, if her supposition were true, it would be a privacy violation.

Like Jose when seeing a QR code in public, the lack of available explicit information and her uncertainty about dataveillance workings left her doubtful about whether her supposition of being subjected to dataveillance was justified.

Visibility of Dataveillance Practices in Triggers. Besides dataveillance imaginaries, the visibility of dataveillance practices was a second determinant for triggers where participants felt subjected to dataveillance. In most cases, the visibility of dataveillance practices was in line with the dataveillance imaginaries, which determined whether an everyday life event became a trigger.

The following examples reflect instances where the visibility of dataveillance practices seemed more important than existing dataveillance imaginaries. This was the case when dataveillance practices were overt to participants, that is, when the trigger revealed the kind of data collected and analyzed as well as the method of data collection and analysis. For example, when Katharina was required to disclose the exact date of birth to place an online order, the kind of collected and analyzed data as well as the purpose of the dataveillance practice were explicitly mentioned in the checkout process. Hence, visibility played a central role in this everyday life event triggering her sense of dataveillance.

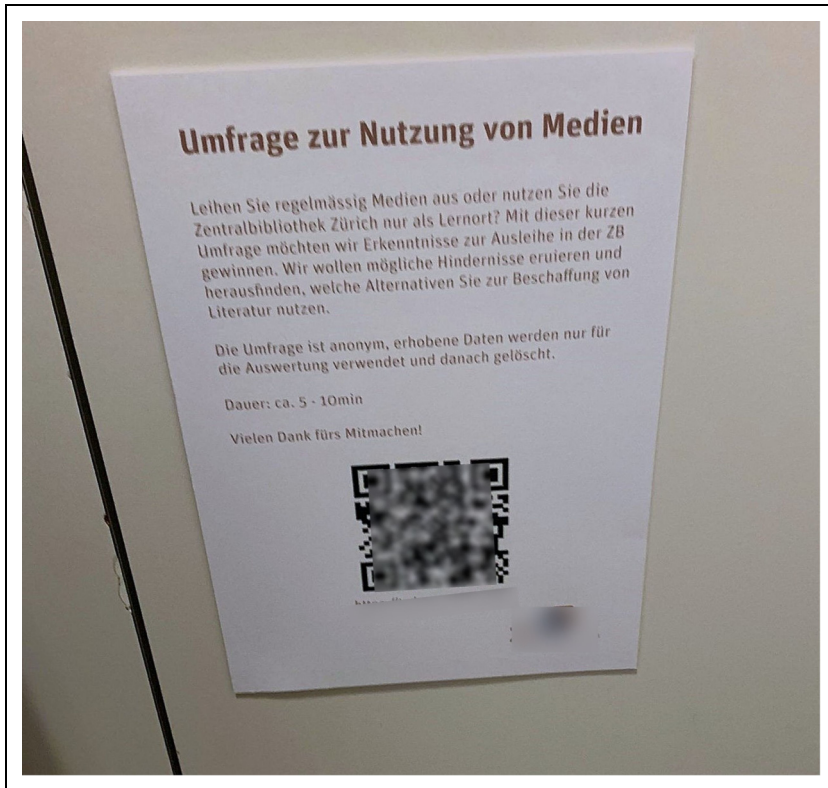


Figure 5. Picture of the QR Code Sent by Katharina.
QR: Quick Response.

In another instance, Katharina saw a QR code to an online survey on a sign in a public library as shown in Figure 5.

She commented:

Data are explicitly collected in this library to find out which methods users employ for media procurement.

In contrast with Jose's encounter with a QR code where dataveillance practices were not visible due to a lack of information, the sign provided explicit information about the trigger-initiating actor (the public library), the purpose of data collection and analysis (gaining insights into how people obtain media from the library), and the handling of the collected data (data are anonymized, analyzed only for the stated purpose, and then deleted). Although she did not scan the code, Katharina anticipated being subjected to dataveillance if she had done so due to the overt visibility of dataveillance practices.

Conclusion

This study mapped the triggers of a sense of dataveillance and explored from a user perspective (1) what the triggers of a sense of dataveillance are and how they can be characterized and (2) which everyday life events become triggers and why.

Our findings show that first, the reported online and offline triggers are characterized by the perceived trigger-initiating actors. These triggers are deeply embedded in all aspects of everyday life. This characterization can inform future empirical studies investigating individual differences in forming and experiencing a sense of dataveillance and its consequences. Second, we found that everyday life events become triggers of a sense of dataveillance while consuming information about dataveillance or while feeling subjected to dataveillance. This mirrors the distinction between surveillance beliefs into information-driven and experience-driven beliefs by Strycharz and Segijn (2022) and therefore provides further insight into the interconnection of triggers and dataveillance imaginaries. Our research adds to literature on a sense of dataveillance by showing that individuals can feel that either they are or that someone else is subjected to dataveillance. This feeling can be either immediate or anticipated, highlighting a temporal dimension in perceiving dataveillance.

Furthermore, our analysis revealed individual differences regarding which everyday life events become triggers. The common determinant of whether everyday life events became triggers was individuals' dataveillance imaginaries. Events became triggers when they connected to imaginaries about the actors, workings, data types, and consequences of dataveillance (Kappeler et al., 2023).

Additionally, the visibility of dataveillance practices also determined whether everyday life events, in which individuals felt subjected to dataveillance, became triggers. This was the case when the kind of collected and analyzed data, and the method of data collection and analysis were overtly visible.

We also found that participants experienced negative feelings with triggers when the perceived intrusiveness of dataveillance was not proportionate to its purpose which relates to the privacy calculus (Plangger & Montecchi, 2020), when users were not certain about the workings of dataveillance, and when user agency was low.

Although participants provided additional information about the triggers, follow-up interviews would have been beneficial for nuanced context of reported triggers. A further limitation is the high proportion of users with self-reported high internet skills, high education levels, and young age in the sample. While the sample reflects the skill level of the Swiss population (Latzer et al., 2023a), it includes users who likely have greater digital and algorithmic literacy (e.g., Bachmann & Hertweck, 2025; Kappeler, 2024) and already are more sensitized to dataveillance practices, potentially making them more sensitive to certain triggers, e.g., personalized ads (Boerman & Segijn, 2022; Segijn & van Ooijen, 2020). While this bias should be acknowledged, the findings remain valuable for mapping triggers of a sense of dataveillance among digitally engaged users, with similar patterns expected in other sociodemographic groups. Nonetheless, future research should include less skilled, less educated, and older users to assess differences across groups, which are plausible as sociodemographic backgrounds and digital media use influence how people encounter and make sense of digital technologies and data (Das, 2024). The sample bias in this study likely stems from the recruitment strategy (i.e., online ad dissemination), and the study's framing as an opportunity to actively contribute to research. This may have led to a self-selection bias of skilled, highly educated, and young internet users. To recruit a more diverse sample, future studies could offer nondigital formats, such as pen-and-paper diaries, and recruit offline through community centers, senior organizations, or institutions for continuing education.

A methodological limitation of this diary study is slight respondent fatigue (Bartlett & Milligan, 2015), reflected in shorter or less frequent trigger reports by some participants toward the end of the study. However, most participants continued reporting previously experienced triggers. This sustained engagement was likely supported by the participation requirement of interest in internet-related topics and the regular reminders from the research team.


This article provides several contributions to research on the formation of a sense of dataveillance and chilling effects. Empirical research on the triggers of a sense of dataveillance is essential for the understanding of chilling effects because triggers initiate the causal mechanism of chilling effects (Büchi et al., 2023). This study provides an innovative user-centered approach to empirical research on triggers, allowing for expansive open answers from a user perspective instead of predefining specific triggers. This revealed that extant literature has not exhaustively discussed different types of triggers (e.g., observation of privacy measures) which is essential for thoroughly investigating the sense of dataveillance and its consequences. Our characterization of triggers therefore provides a basis for further empirical research exploring the effects of specific everyday life events.


Furthermore, the in situ study design minimized the recall bias, a common methodological challenge in chilling effects research where effects are likely small (Büchi et al., 2023). The characteristics we found for the triggers of a sense of dataveillance as well as the determinants of such triggers lend themselves to further empirical analyses (e.g., as experimental stimuli) or can form the basis for hypotheses regarding differences in experiencing chilling effects.


Our findings invite reflection on the structural conditions under which triggers are experienced and how they are embedded in broader economic structures. As imaginaries are not only subjective but also socially grounded (Bucher, 2017; Kappeler et al., 2023), triggers are also shaped by the social, cultural, and political context in which they occur. They reflect broader structural asymmetries in the digital ecosystem, particularly between users and corporate actors with often opaque data practices. The feelings of being watched, tracked, or profiled expressed by participants resonate with dynamics characteristic of surveillance capitalism (Zuboff, 2019), in which user data are commodified and used to predict and influence behavior, often without meaningful consent or transparency (e.g., Couldry & Mejias, 2019). Participants' reports often conveyed mistrust, uncertainty, or perceived loss of control, indicating an implicit awareness of these imbalances. The reported triggers thus can be seen as everyday reflections of data practices that position users primarily as sources of information.


This article also contributes to the governance of dataveillance practices aiming to constrain undesired and promote desired consequences. This is central considering the lacking consensus in literature about whether triggers should be kept covert to prevent undesired consequences like chilling effects (Büchi et al., 2022) or if they should be prominent to increase people's awareness and foster dataveillance literacy (Degeling et al., 2019). For instance, policies requiring websites and platforms to disclose their data policies with pop-up notifications aim to keep the users' sense of dataveillance at a high level and sensitize them to dataveillance practices which can facilitate people's autonomous management of their privacy (Degeling et al., 2019). Similarly, design efforts of websites and platforms are intended to disclose how personal information is used in ad generation to increase transparency of targeted ads (Barbosa et al., 2021; Kim et al., 2019). On the other hand, to prevent inhibitory effects on digital communication behavior, users' sense of dataveillance should remain at a lower level (Büchi et al., 2022), which suggests keeping triggers of a sense of dataveillance covert. Such conflicts of interest need to be addressed with an appropriate understanding of potential differences in the everyday life events becoming triggers of a sense of dataveillance.

ORCID iDs

Céline Odermatt  <https://orcid.org/0009-0004-6967-9813>

Noemi Festic  <https://orcid.org/0000-0002-3918-3639>

Daniela Jaramillo-Dent  <https://orcid.org/0000-0001-8372-0107>

Kiran Kappeler  <https://orcid.org/0000-0003-2807-4012>

Ethical Statement

All participants were informed of the study's objective and gave written informed consent for their voluntary participation and for the analysis of their anonymized data for publication purposes. The study complies with the fundamental principles of research ethics in the humanities and social sciences, particularly regarding privacy and the confidential handling of data. According to the University of Zurich Ethics Commission, this study did not require further ethics approval because it did not meet any of the conditions for additional review, that is, the involvement of sensitive data or vulnerable participants, or the potential for harm or disadvantage to participants.

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 Swiss National Science Foundation (Grant 201176).

Declaration of Conflicting Interests

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

Data Availability

The research material used for this article is available on Figshare (<https://figshare.com/s/71568cdcac8d8d53458>).

Note

1. The Figshare page can be found here: <https://figshare.com/s/71568cdcac8d8d53458>.

References

- Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox. *Journal of Retailing*, 91(1), 34–49 <https://doi.org/10.1016/j.jretai.2014.09.005>
- Arcangeli, M. (2019). *Supposition and the imaginative realm*. Routledge.
- Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2018). Paradoxical effects of self-awareness of being observed. *Journal of Experimental Criminology*, 14(1), 19–47 <https://doi.org/10.1007/s11292-017-9311-5>
- Bachmann, R., & Hertweck, F. (2025). The gender gap in digital literacy: A cohort analysis for Germany. *Applied Economics Letters*, 32(5), 608–613 <https://doi.org/10.1080/13504851.2023.2277685>
- Barbosa, N. M., Wang, G., Ur, B., & Wang, Y. (2021). Who am I? A design probe exploring real-time transparency about online and offline user profiling underlying targeted ads. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 5(3), 1–32 <https://doi.org/10.1145/3478122>
- Bartlett, R., & Milligan, C. (2015). *What is diary method?* London, UK: Bloomsbury Academic.
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior. *Communication Research*, 48(7), 953–977 <https://doi.org/10.1177/0093650218800915>
- Boerman, S. C., & Segijn, C. M. (2022). Awareness and perceived appropriateness of synced advertising in Dutch adults. *Journal of Interactive Advertising*, 22(2), 187–194 <https://doi.org/10.1080/15252019.2022.2046216>
- Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, 20(1), 30–44. <https://doi.org/10.1080/1369118X.2016.1154086>

- Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society*, 9(1), 1–14 <https://doi.org/10.1177/20539517211065368>
- Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., & Velidi, S. (2023). Making sense of algorithmic profiling: User perceptions on Facebook. *Information, Communication & Society*, 26(4), 809–825 <https://doi.org/10.1080/1369118X.2021.1989011>
- Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling. *Computer Law & Security Review*, 36, 1–39 <https://doi.org/10.1016/j.clsr.2019.105367>
- Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–512 <https://doi.org/10.1145/42411.42413>
- Clarke, R. (2019). Risks inherent in the digital surveillance economy. *Journal of Information Technology*, 34(1), 59–80 <https://doi.org/10.1177/0268396218815559>
- Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336–349 <https://doi.org/10.1177/1527476418796632>
- Das, R. (2024). Data reflexivity as work-in-progress: A relational, life-course approach to people's encounters with datafication. *Convergence*, 30(6), 1939–1958 <https://doi.org/10.1177/13548565241270889>
- Dear, K., Dutton, K., & Fox, E. (2019). Do 'watching eyes' influence antisocial behavior? *Evolution and Human Behavior*, 40(3), 269–280 <https://doi.org/10.1016/j.evolhumbehav.2019.01.006>
- Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy ... now take some cookies: Measuring the GDPR's impact on web privacy. In *Proceedings 2019 Network and Distributed System Security Symposium (NDSS)* (pp. 1–20). San Diego, CA: NDSS.
- Dev, J., Moriano, P., & Camp, L. J. (2020). Lessons learnt from comparing WhatsApp privacy concerns across Saudi and Indian populations. In *Proceedings of the Sixteenth Symposium on Usable Privacy and Security* (pp. 81–97). Berkeley, CA: USENIX. <https://www.usenix.org/system/files/soups2020-dev.pdf>.
- DeVito, M. A., Gergle, D., & Birnholtz, J. (2017). "Algorithms ruin everything": #RIPTwitter, folk theories, and resistance to algorithmic change in social media. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 3163–3174). New York, NY: ACM. <https://dl.acm.org/doi/10.1145/3025453.3025659>
- Dogrul, L. (2021). Folk theories of algorithmic operations during internet use. *The Information Society*, 37(5), 287–298 <https://doi.org/10.1080/01972243.2021.1949768>
- Festic, N. (2022). Same, same, but different! qualitative evidence on how algorithmic selection applications govern different life domains. *Regulation & Governance*, 16(1), 85–101 <https://doi.org/10.1111/rego.12333>
- Frick, N. R. J., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications*, 47, 1–16. <https://doi.org/10.1016/j.elerap.2021.101046>
- Grigorios, L., Magrizos, S., Kostopoulos, I., Drossos, D., & Santos, D. (2022). Overt and covert customer data collection in online personalized advertising: The role of user emotions. *Journal of Business Research*, 141, 308–320 <https://doi.org/10.1016/j.jbusres.2021.12.025>
- Herder, E., & Zhang, B. (2019). Unexpected and unpredictable: Factors that make personalized advertisements creepy. In *Proceedings of the 23rd International Workshop on Personalization and Recommendation on the Web and Beyond* (pp. 1–6). New York, NY: ACM. <https://doi.org/10.1145/3345002.3349285>.
- Hu, X., & Sastry, N. (2019). Characterising third party cookie usage in the EU after GDPR. In *Proceedings of the 10th ACM Conference on Web Science* (pp. 137–141). New York, NY: ACM. <https://doi.org/10.1145/3292522.3326039>

- Jansen, A. M., Giebels, E., van Rompay, T. J. L., & Junger, M. (2018). The influence of the presentation of camera surveillance on cheating and pro-social behavior. *Frontiers in Psychology*, 9, 1–12. <https://doi.org/10.3389/fpsyg.2018.01937>
- Kappeler, K. (2024). A longitudinal perspective on digital skills for everyday life: Measurement and empirical evidence. *Media and Communication*, 12, 1–18. <https://doi.org/10.17645/mac.8159>
- Kappeler, K., Festic, N., & Latzer, M. (2023). Dataveillance imaginaries and their role in chilling effects online. *International Journal of Human-Computer Studies*, 179, 1–15. <https://doi.org/10.1016/j.ijhcs.2023.103120>
- Kapsch, P. H. (2022). Exploring user agency and small acts of algorithm engagement in everyday media use. *Media International Australia*, 183(1), 16–29. <https://doi.org/10.1177/1329878X211067803>
- Kelly, N. (2022). Facing surveillance: Personified surveillance, algorithmic injustice, and the myth of big brother in post-Snowden popular culture. *Surveillance & Society*, 20(2), 172–185. <https://doi.org/10.24908/ss.v20i2.14492>
- Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, 45(5), 906–932. <https://doi.org/10.1093/jcr/ucy039>
- Kind, A. (2016). Exploring imagination. In A. Kind (ed) *The Routledge Handbook of Philosophy of Imagination* (pp. 1–12). London, UK: Routledge.
- Kruglanski, A. W. (1990). Lay epistemic theory in social-cognitive psychology. *Psychological Inquiry*, 1(3), 181–197. https://doi.org/10.1207/s15327965pli0103_1
- Latzer, M. (2022). The digital Trinity—Controllable human evolution—Implicit everyday religion. *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, 74(1), 331–354. <https://doi.org/10.1007/s11577-022-00841-8>
- Latzer, M., Festic, N., Kappeler, K., & Odermatt, C. (2023a). *Internetverbreitung und digitale Bruchlinien in der Schweiz 2023 [Internet penetration and digital divides in Switzerland 2023]*. Zurich, CH: University of Zurich. https://mediachange.ch/media/pdf/publications/Verbreitung_und_Bruchlinien_2023_.pdf
- Latzer, M., Festic, N., Kappeler, K., & Odermatt, C. (2023b). *Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2023 [Trust and concerns regarding internet use in Switzerland 2023]*. Zurich, CH: University of Zurich. https://www.mediachange.ch/media/pdf/publications/Vertrauen_Sorgen_2023_.pdf
- Lupton, D., & Michael, M. (2017). Depends on who's got the data': Public understandings of personal digital dataveillance. *Surveillance & Society*, 15(2), 254–268. <https://doi.org/10.24908/ss.v15i2.6332>
- Lyon, D. (2022). Surveillance. *Internet Policy Review*, 11(4), 1–19 <https://doi.org/10.14763/2022.4.1673>
- Manesi, Z., Van Lange, P. A. M., & Pollet, T. V. (2016). Eyes wide open: Only eyes that pay attention promote prosocial behavior. *Evolutionary Psychology*, 14(2), 1–15. <https://doi.org/10.1177/1474704916640780>
- Meredith, J. (2016). Transcribing screen-capture data. *International Journal of Social Research Methodology*, 19(6), 663–676. <https://doi.org/10.1080/13645579.2015.1082291>
- Nasiopoulos, E., Risko, E. F., Foulsham, T., & Kingstone, A. (2015). Wearable computing: Will it make people prosocial? *British Journal of Psychology*, 106(2), 209–216. <https://doi.org/10.1111/bjop.12080>
- Neisser, U. (1978). Perceiving, anticipating, and imagining. In C. W. Savage (ed) *Perception and Cognition Issues in the Foundations of Psychology* (pp. 89–105). Minneapolis, MN: University of Minnesota Press. <https://hdl.handle.net/11299/185331>
- Obar, J. A., & 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. <https://doi.org/10.1080/1369118X.2018.1486870>
- Penney, J. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, 31(1), 117–182. <https://doi.org/10.15779/Z38SS13>
- Penney, J. (2022). Understanding chilling effects. *Minnesota Law Review*, 106(3), 1451–1530. <https://minnesotalawreview.org/article/understanding-chilling-effects/>

- Penney, J., Citron, D. K., & Ingber, A. S. (2025). The chilling effects of dobbs. *Florida Law Review*, 77(2), 357–416. <https://scholarship.law.ufl.edu/flr/vol77/iss2/1>
- Petty, R., & Briñol, P. (2014). Emotion and persuasion: Cognitive and meta-cognitive processes impact attitudes. *Cognition and Emotion*, 29(1), 1–26. <https://doi.org/10.1080/02699931.2014.967183>
- Petty, R., Briñol, P., & Tormala, Z. (2002). Thought confidence as a determinant of persuasion. *Journal of Personality and Social Psychology*, 82(5), 722–741. <https://doi.org/10.1037/0022-3514.82.5.722>
- Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing*, 50, 32–44. <https://doi.org/10.1016/j.intmar.2019.10.004>
- Plantin, J.-C., & Punathambekar, A. (2019). Digital media infrastructures: Pipes, platforms, and politics. *Media, Culture & Society*, 41(2), 163–174. <https://doi.org/10.1177/0163443718818376>
- Puppis, M. (2019). Analyzing talk and text I: Qualitative content analysis. In H. Van den Bulck, M. Puppis, K. Donders, & L. Van Audehove (Eds.), *The Palgrave Handbook of Methods for Media Policy Research* (pp. 367–384). Cham, CH: Springer.
- Robinson, S. C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 214–233. <https://doi.org/10.1080/10919392.2018.1482601>
- Segijn, C. M., Strycharz, J., Riegelman, A., & Hennesy, C. (2021). A literature review of personalization transparency and control: Introducing the transparency–awareness–control framework. *Media and Communication*, 9(4), 120–133. <https://doi.org/10.17645/mac.v9i4.4054>
- Segijn, C. M., Strycharz, J., Turner, A., & Oprea, S. J. (2025). My phone must be listening!": Peoples' surveillance beliefs around devices "listening" to offline conversations in the US, The Netherlands, and Poland. *Big Data & Society*, 12(2): 1–15. <https://doi.org/10.1177/20539517251337102>
- Segijn, C. M., & 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. <https://doi.org/10.1089/cyber.2019.0682>
- Shankar, A., Yadav, R., Behl, A., & Gupta, M. (2021). How does dataveillance drive consumer online payment resistance? *Journal of Consumer Marketing*, 40(2), 224–234. <https://doi.org/10.1108/JCM-03-2021-4555>
- Siles, I., Espinoza-Rojas, J., Naranjo, A., & Tristán, M. F. (2019). The mutual domestication of users and algorithmic recommendations on Netflix. *Communication, Culture and Critique*, 12(4), 499–518. <https://doi.org/10.1093/ccc/tcz025>
- Siles, I., Segura-Castillo, A., Solís, R., & Sancho, M. (2020). Folk theories of algorithmic recommendations on spotify. *Big Data & Society*, 7(1), 1–15. <https://doi.org/10.1177/2053951720923377>
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–560. <https://doi.org/10.2307/40041279>
- Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903. <https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/>.
- Spottswood, E. (2017). Influencing privacy on social network sites [Doctoral dissertation, Cornell University]. eCommons. <https://ecommons.cornell.edu/handle/1813/38806>.
- Stavraki, M., Lamprinakos, G., Briñol, P., Petty, R., Karantinou, K., & Díaz, D. (2021). The influence of emotions on information processing and persuasion. *Journal of Experimental Social Psychology*, 93, 1–16. <https://doi.org/10.1016/j.jesp.2020.104085>
- 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), 296–311. <https://doi.org/10.1177/1077699016630255>
- Stoycheff, E. (2023). Cookies and content moderation: Affective chilling effects of internet surveillance and censorship. *Journal of Information Technology & Politics*, 20(2), 113–124. <https://doi.org/10.1080/19331681.2022.2063215>

- Strycharz, J., Kim, E., & Segijn, C. M. (2022). Why people would (not) change their media use in response to perceived corporate surveillance. *Telematics and Informatics*, 71, 1–15. <https://doi.org/10.1016/j.tele.2022.101838>
- Strycharz, J., & Segijn, C. M. (2022). The future of dataveillance in advertising theory and practice. *Journal of Advertising*, 51(5), 574–591. <https://doi.org/10.1080/00913367.2022.2109781>
- Strycharz, J., & Segijn, C. M. (2024). Ethical side-effect of dataveillance in advertising: Impact of data collection, trust, privacy concerns and regulatory differences on chilling effects. *Journal of Business Research*, 173, 1–13. <https://doi.org/10.1016/j.jbusres.2023.114490>
- Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019a). Consumer view on personalized advertising: Overview of self-reported benefits and concerns. In E. Bigne & S. Rosengren (eds) *Advances in Advertising Research X* (pp. 53–66). Wiesbaden, DE: Springer.
- Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019b). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology*, 13(2), 1–13. <https://doi.org/10.5817/CP2019-2-1>
- Tormala, Z. L., Rucker, D. D., & Seger, C. R. (2008). When increased confidence yields increased thought: A confidence-matching hypothesis. *Journal of Experimental Social Psychology*, 44(1), 141–147. <https://doi.org/10.1016/j.jesp.2006.11.002>
- van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- Vanover, C., Mihas, P., & Saldaña, J. (2022). *Analyzing and interpreting qualitative research*. Thousand Oaks, CA: Sage.
- van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283–297. <https://doi.org/10.1016/j.chb.2017.10.007>
- White, G. L., & Zimbardo, P. G. (1975). The chilling effects of surveillance: Deindividuation and reactance (Report No. ADA013230). Defense Technical Information Center. <https://apps.dtic.mil/sti/citations/ADA013230>.
- Ytre-Arne, B., & Moe, H. (2021). Folk theories of algorithms: Understanding digital irritation. *Media, Culture & Society*, 43(5), 807–824. <https://doi.org/10.1177/0163443720972314>
- Zhang, D., Boerman, S. C., Hendriks, H., Araujo, T., & Voorveld, H. (2023). A peak into individuals' perceptions of surveillance. In A. Vignolles & M. K. J. Waiguny (eds) *Advances in Advertising Research (Vol. XII): Communicating, Designing and Consuming Authenticity and Narrative* (pp. 163–178). Wiesbaden, DE: Springer.
- Zhang, D., Boerman, S. C., Hendriks, H., Goot, M. J. v. d., Araujo, T., & Voorveld, H. (2024). They know everything”: Folk theories, thoughts, and feelings about dataveillance in media technologies. *International Journal of Communication*, 18(2024), 2710–2730. <https://ijoc.org/index.php/ijoc/article/view/21495>
- Zuboff, S. (2019). *The age of surveillance capitalism*. New York, NY: PublicAffairs.