International Journal of Communication 18(2024), 2710-2730 1932–8036/20240005

"They Know Everything": Folk Theories, Thoughts, and Feelings About Dataveillance in Media Technologies

DONG ZHANG♦[1]
University of Amsterdam, The Netherlands

SOPHIE C. BOERMAN
Wageningen University & Research, The Netherlands

HANNEKE HENDRIKS
Radboud University, The Netherlands

MARGOT J. VAN DER GOOT
THEO ARAUJO
HILDE VOORVELD
University of Amsterdam, The Netherlands

Dataveillance refers to the automated, continuous, and unspecific collection, storage, and processing of digital traces. This study explores individuals' perspectives on dataveillance in media technologies by investigating their folk theories, thoughts, and feelings. Through in-depth interviews with participants aged 18 to 86 years, we identified 3 prominent folk theories, which illustrated how individuals make sense of corporate, technology, and state dataveillance. Thoughts and feelings about dataveillance were mixed: Participants perceived a power imbalance, had concerns over unethical practices and their privacy, and found dataveillance violating and creepy; meanwhile, they recognized that dataveillance improved user experiences, brought benefits beyond the realm of technology, and was "smart." More importantly, we identified 4 cognitive coping strategies people used to rationalize their technology use under dataveillance: Resigning, self-

Dong Zhang: d.zhang@uva.nl
Sophie C. Boerman: sophie.boerman@wur.nl
Hanneke Hendriks: hanneke.hendriks@ru.nl
Margot J. van der Goot: M.J.vanderGoot@uva.nl
Theo Araujo: T.B.Araujo@uva.nl
Hilde Voorveld: H.A.M.Voorveld@uva.nl
Date submitted: 2023-04-22

[1] We would like to thank Jeltje Heuperman for her invaluable assistance with recruiting, interviewing, transcribing, and translating part of the interviews.

empowering, downplaying, and sympathizing. These findings offer insights into individuals' beliefs about and responses to dataveillance, providing important implications for policy makers and media literacy programs.

Keywords: dataveillance, surveillance, folk theory, thought, feeling, coping strategy

People today engage in a broader range of digital activities than ever before. These interactions with media technologies continuously generate data about the users, which are collected by companies, governments, and other parties for various purposes. This practice of automatic, continuous, and unspecific collection, storage, and processing of digital traces to regulate or govern the behavior of people or groups is termed *dataveillance* (Büchi, Festic, & Latzer, 2022; Clarke, 1988; Strycharz & Segijn, 2022).

Dataveillance encompasses a plethora of phenomena: The Snowden leaks revealed mass dataveillance by the government (Lyon, 2014); companies collect personal data for algorithmic profiling and targeted advertising (Büchi, Fosch-Villaronga, Lutz, Tamò-Larrieux, & Velidi, 2023); and individuals are being watched on social media by family, educators, and employers (Duffy & Chan, 2019). To individual users, each type of dataveillance may not be equally prominent during their everyday use of media technologies across various contexts. Thus, a cross-context examination can help us identify the salience of various dataveillance phenomena in shaping people's perceptions about dataveillance, leading to the following questions: By whom do individuals think they are being surveilled? For what purposes? And how? As the first aim of this study, we seek the answer to what individual media technology users perceive as the source of dataveillance, and consequently, whether they think these sources hold different purposes and adopt different mechanisms of dataveillance. We then organize how people make sense of these into *folk theories* of dataveillance. Folk theories are developed by individuals based on personal experiences and beliefs (Gelman & Legare, 2011), which richly reflect their subjective conceptualization of the dataveillance system (DeVito, Gergle, & Birnholtz, 2017). Moreover, folk theories function in place of users' factual knowledge about a system, which in turn affects one's dataveillance beliefs and dataveillance responses, regardless of the accuracy of the theories (DeVito et al., 2017; Strycharz & Segijn, 2022). Understanding folk theories of dataveillance is therefore an essential first step to understanding why people form certain thoughts and feelings about dataveillance.

Our second aim is to investigate people's thoughts and feelings about dataveillance practices in media technologies. While folk theories depict one's conception of dataveillance, their thoughts and feelings reflect their evaluations of dataveillance. Numerous studies have probed how individuals perceive specific digital phenomena that involve dataveillance practices, such as personalized advertising (e.g., Strycharz, van Noort, Smit, & Helberger, 2019; Ur, Leon, Cranor, Shay, & Wang, 2012), virtual assistants (e.g., Lau, Zimmerman, & Schaub, 2018; Vimalkumar, Sharma, Singh, & Dwivedi, 2021), and algorithmic communication (e.g., Bucher, 2017; Ytre-Arne & Moe, 2020). One may thus argue that individuals' perceptions of dataveillance can be inferred from these studies of specific practices. However, in real life, individuals engage in multiple media technology activities simultaneously (Voorveld, Segijn, Ketelaar, & Smit, 2014), therefore possibly experiencing various types of dataveillance at the same time. This calls for research that identifies shared perceptions of dataveillance across everyday media use contexts for a holistic understanding. Using the privacy calculus as a starting point, we uncover the mixed sentiments people have

about dataveillance and seek explanations for people's continued use of media technologies despite dataveillance. This understanding of folk theories, thoughts, and feelings about dataveillance offers valuable insights for policy makers and media literacy programs. Given the exploratory nature of the study, the findings may also inspire theory advancements in the impact of dataveillance on individuals.

Folk Theories of Dataveillance

Folk Theories as a Framework

Folk theories are "intuitive, informal theories that individuals develop to explain the outcomes, effects, or consequences of technological systems" (DeVito et al., 2017, p. 3165). Gelman and Legare (2011) have pointed out the broad implications of folk theories as they "organize experience, generate inferences, guide learning, and influence behavior and social interaction" (p. 380). What one believes as their folk theory can have profound impacts on their responses to dataveillance and persuasive messages produced through dataveillance (Strycharz & Segijn, 2022). Moreover, folk theories evolve constantly as one continues to interact with technological systems and receive new information, which then guides their further responses to the systems (DeVito, Birnholtz, Hancock, French, & Liu, 2018).

Folk theories as a framework have been applied particularly fruitfully in researching perceptions of algorithms. Folk theories of algorithms range in their specificity from abstract to operational (DeVito et al., 2017). Some theories describe what algorithms are and what they do to media experiences, which are confining, practical, reductive, intangible, and exploitative (Ytre-Arne & Moe, 2020). Some focus on how algorithms work in a particular (e.g., online dating) context (Huang, Hancock, & Tong, 2022). Other folk theories reflect the perceived roles of algorithms: The Spotify algorithm is seen as a social being and a computational machine by its users in Costa Rica (Siles, Segura-Castillo, Solís, & Sancho, 2020); the algorithm of Zhihu, a Chinese question-answer platform, is both an evictor and a protector in the eyes of its gay men users (Zhao, 2023).

Another notion that guided research in this field is *imaginaries*, which refers to how individuals "imagine, perceive, and experience technological phenomena and what these imaginations make possible" (Bucher, 2017, p. 31). Bucher (2017) introduced algorithmic imaginaries and argued their influence on moods and sensations and how these could in turn reshape algorithms. Within the realm of dataveillance, imaginaries are used to understand how (young) people anticipate dataveillance by various social institutions (Duffy & Chan, 2019), as well as the imagined actors, workings, data types, and consequences of dataveillance (Kappeler, Festic, & Latzer, 2023). While our study is rooted in folk theories, it is worth noting that both approaches are valuable in exploring how people conceptualize dataveillance and should be considered when reviewing the relevant literature.

Dimensions of Folk Theories of Dataveillance

Both critical discussions and empirical studies often identify three dimensions of dataveillance: Source, purpose, and mechanism (e.g., Christin, 2020; Kappeler et al., 2023; Lupton & Michael, 2017; Lyon, 2009; Marx, 2015; Zhang, Boerman, Hendriks, Araujo, & Voorveld, 2023). Therefore, we inquire into folk theories of dataveillance using these three dimensions as the guiding structure.

Perceived Source of Dataveillance

The perceived source of dataveillance concerns individuals' perceptions of who (or what) is surveilling them. Multiple studies centering around the Snowden leaks discussed dataveillance by the government (Bakir, Cable, Dencik, Hintz, & McStay, 2015; Dencik & Cable, 2017; Fuchs & Trottier, 2017). With the burgeoning commodification of personal data, dataveillance by commercial companies has received increased scholarly attention (Andrejevic, 2014; Turow, 2021; Zuboff, 2019). Likewise, individuals also identify commercial and government actors as the sources of dataveillance (Kalmus, Bolin, & Figueiras, 2022; Lupton & Michael, 2017). In addition, as Humphreys (2011) suggests, other individuals (e.g., family, educators, and future employers) can also be perceived as sources of dataveillance (Duffy & Chan, 2019; McEwan & Flood, 2018). Furthermore, Guzman (2019) found that people perceive themselves as communicating directly with the technology when using voice-based mobile virtual assistants, indicating that besides humans, artificial intelligence can also be seen as a source of communication. Siles and colleagues (2020) inquired about folk theories of algorithmic recommendations on Spotify and found that people commonly *personify* Spotify as a surveillant "buddy," suggesting the possibility of technology being perceived as not only a source of communication but also a source of dataveillance.

Perceived Purpose of Dataveillance

The perceived purpose of dataveillance explains *why* the perceived source conducts dataveillance practices according to media technology users. While academia defines dataveillance as a purposeful action to influence, manage, or manipulate (Lyon, 2009; Susser, Roessler, & Nissenbaum, 2019), individuals as the subjects of dataveillance might perceive different purposes. Lupton and Michael (2017) mentioned that individuals identified commercial, security, or government-related purposes of dataveillance. Scholars have raised the notion of *surveillance capitalism*, meaning that companies make profits and accumulate capital through dataveillance (Fuchs, 2011; Zuboff, 2019). Governments also use digital dataveillance data for national security purposes (van Dijck, 2014). Moreover, dataveillance is also used for research, health, and employee management (Carver & Mackinnon, 2020; Stanton & Stam, 2003; van Dijck, 2014).

Perceived Mechanism of Dataveillance

The perceived mechanism of dataveillance is how individuals think dataveillance is conducted. Previous research has found that individuals have a limited understanding of how dataveillance is enabled through media technologies (Lupton & Michael, 2017). Nevertheless, consumer reports, news articles, and social media content suggest that certain perceived mechanisms exist. For example, 43% of smartphone owners in the United States believe that phones are constantly listening to collect data for targeted ads (Fowler, 2019).

Taking the three dimensions of dataveillance into account, we ask the following research question:

RQ1: What are the (a) perceived sources, (b) perceived purposes, and (c) perceived mechanisms of dataveillance, and how do they collectively form the folk theories of dataveillance?

Thoughts and Feelings About Dataveillance

The second aim of this study is to investigate what people think and feel about dataveillance in media technologies. In the literature, dataveillance has usually been given a negative connotation (e.g., Fuchs, 2011; Zuboff, 2019). However, what individuals perceive about dataveillance practices can be both positive and negative as the privacy calculus posits that individuals calculate the perceived costs and benefits of disclosing personal information, which then guide the behavior of privacy disclosure (Dinev & Hart, 2006). Based on the model, we expect to observe both perceived costs and benefits by users of dataveillance-enabling media technologies. Whereas traditionally privacy calculus is regarded as a fully rational process, according to Kehr, Kowatsch, Wentzel, and Fleisch (2015), privacy calculus is also influenced by momentary affective states. This indicates that feelings as affective evaluations may also play a role in the privacy calculus. Therefore, in this study, we investigate both thoughts and feelings about dataveillance.

Multiple positive thoughts and feelings have been covered in previous studies. Since many dataveillance practices involve using personal data for personalization, the perceived relevance of such communication messages is widely appreciated by individuals (Jung, 2017; Kim & Huh, 2017; Strycharz et al., 2019). Emotionally, personalized advertisements resulting from well-balanced corporate surveillance give consumers a pleasurable feeling of recognition and enjoyment (Ruckenstein & Granroth, 2020). Users also appreciate the convenience brought by dataveillance practices such as personalized advertising and voice assistants (Lau et al., 2018; Strycharz et al., 2019). Additionally, Ur and colleagues (2012) found that individuals think online behavioral advertising is useful and smart. Usefulness is also perceived by users of voice-based digital assistants (Vimalkumar et al., 2021). Another positive aspect of dataveillance comes from its enablement of self-tracking, which gives people the opportunity for self-exploration (Kristensen & Ruckenstein, 2018).

On the other hand, negative thoughts and feelings also exist among individuals. Studies have revealed that individuals are concerned about their privacy when they are involved in dataveillance practices (Smit, van Noort, & Voorveld, 2014). In prior studies, participants have mentioned that dataveillance using personal digital data is scary (Lupton & Michael, 2017) and creepy (Phelan, Lampe, & Resnick, 2016; Ur et al., 2012). Lastly, people are also irritated and annoyed by algorithms (Ytre-Arne & Moe, 2020).

Most of the studies above focused on specific dataveillance practices. However, in real life, people experience multiple types of dataveillance simultaneously, and how they think and feel about it across different contexts remains unknown. The following research question is thus posed:

RQ2: What are people's thoughts and feelings about dataveillance in media technologies?

Methods

Given the exploratory nature of the research questions, qualitative in-depth interviewing was considered the ideal research method. In interviews, participants are given the opportunity to share information in their own words and elaborate freely, which provides rich and detailed answers to the research questions (Braun & Clarke, 2013).

Participants

To capture diverse folk theories, thoughts, and feelings, we purposefully selected participants who varied in technology use, age, gender, and education, following the maximum variation sampling strategy (Patton, 2015). Participants were recruited through the authors' acquaintances and their social circles (e.g., friends of friends). None of the participants had close interpersonal relationships with the interviewers. To avoid priming effects, the research aim was framed as gathering people's daily experiences with digital technologies, with the incentive of a €25 prize draw. In total, 23 Dutch adults were interviewed, including 11 females and 12 males aged between 18 and 86 years. These participants had used four to eight types of common consumer technologies in the month prior to their participation. The education levels ranged from low to high, while in general, they were relatively high. Most participants worked or studied in areas that do not require extensive knowledge of information technologies, for example, health care, real estate, and logistics, while a few people worked with information technologies more frequently in roles like Web developer and digital designer. Participants' Internet skills were measured using the Internet Skills Scale on a 7-point scale (van Deursen, Helsper, & Eynon, 2016) and ranged between medium and high levels. All participants lived in the Netherlands.[2]

Interviews

Before the interviews and after providing informed consent, participants filled in their demographic information, technology use, and their preferred interview language in a questionnaire. Fourteen participants were interviewed by the first author in English. The rest were interviewed by a research assistant in Dutch. All interviews were held and recorded online using Zoom due to COVID-19 constraints between January and March 2021. The recordings were then transcribed verbatim. Following methodological recommendations by Squires (2009), the transcripts in Dutch were translated into English by the same research assistant, whose native language is Dutch and who is proficient in English. All transcripts were then analyzed in English.

The interview guide contained three topics. Topic 1 explored dataveillance episodes (see Strycharz & Segijn, 2022). Participants were first asked to elaborate on their technology use habits based on their answers to the questionnaire. Next, participants had to describe some experiences where they felt watched, listened to, or recorded when using media technologies. For each experience, the interviewers further probed the perceived sources, purposes, and mechanisms of dataveillance to form the folk theories (Topic 2) and thoughts and feelings about the dataveillance episodes (Topic 3). Since the words "dataveillance" and "surveillance" might have negative connotations in public discourse, neither of them was used in any interviews. We were also aware that simply asking participants to recall a situation where they felt watched could also make the negative thoughts and feelings more prominent than the positive ones. To minimize such influence, we purposefully always discussed folk theories first and asked about thoughts and feelings afterward.

The interview guide was continuously adapted throughout the data collection process in accordance with the grounded theory approach (Charmaz, 2014). While analyzing the earlier interviews, certain patterns

[2] An overview of participants' demographic information can be found at https://osf.io/tczva.

began to emerge, which made us rethink and adapt the interview guide to inform the research questions better. For instance, multiple participants mentioned that they were aware of certain dataveillance practices but did not feel watched. We adapted the interview guide to inquire why they did not feel surveilled in such situations, and in later interviews, we asked for situations where participants observed data collection taking place but did not necessarily feel watched.

Data Analysis

Guided by grounded theory, the data collection, transcription, coding, and analysis stages for different interviews happened simultaneously until we reached data saturation (Charmaz, 2014). Moreover, we employed the constant comparative method by continuously reviewing and comparing original transcripts, emerging codes, categories, and concepts to ensure the complexity of the data was well-captured (Glaser & Strauss, 1967). Memo writing was used to record thoughts that occurred during analyses for continuous refinement.

We conducted data analysis using the ATLAS.ti software. The first step was initial coding, where the researcher scrutinized the transcripts and assigned open codes to discrete parts of the data. The concepts that were identified in earlier research served as sensitizing concepts, that is, concepts that gave us initial but tentative ideas during the initial coding. In the second step (focused coding), the initial codes were synthesized and grouped into categories using the grouping function in ATLAS.ti. Third, theoretical coding was conducted using the visual network function in the software, where the researchers identified the relationships among perceived sources, purposes, and mechanisms to form the folk theories, as well as the relationships between the dimensions of folk theories and thoughts and feelings of dataveillance.

Results

Dataveillance Episodes

As we intentionally did not confine dataveillance to a particular context, participants could think freely of instances where they felt, observed, or assumed data collection, namely the dataveillance episodes. These dataveillance episodes provided contexts for the following discussions of folk theories, thoughts, and feelings. The most common dataveillance episode was seeing online advertisements that participants believed to be based on their online (e.g., past searches) or offline (e.g., real-life conversations) behaviors. Another often mentioned dataveillance episode was getting personalized recommendations from digital services such as Spotify and Google Maps[3].

Perceived Sources

Various sources of dataveillance were mentioned during the interviews, which can be categorized into four categories: *Commercial companies, technologies, government*, and the *unknown source "they."*

[3] A complete list of dataveillance episodes can be found at https://osf.io/9b8wa.

Commercial companies were the most commonly perceived source. Participants perceived the source to be either companies in general: "just businesses or companies" (P2), or specifically the big tech companies: "There's Google behind it, and there's Microsoft. Those big guys are behind it" (P13). In many other cases, participants directly pointed out the specific companies involved in their dataveillance episodes, such as the owners of the services they used or companies that tried to persuade them. For example, when P17 saw an advertisement on Facebook about a clothing app, she perceived both Facebook and the clothing app to be the sources of dataveillance.

Technologies that were directly involved in the dataveillance episodes were also perceived as sources of dataveillance. People believed that the algorithms in the systems as well as the devices and services being used (e.g., laptops, smartphones, Web browsers) were monitoring them, but they did not attribute agency to the technologies. Instead, they articulated that the technologies were ultimately controlled by companies while perceiving dataveillance as coming directly from the technologies.

Sometimes, participants viewed *governments* as potential sources of dataveillance. Participants believed that governments could monitor the pandemic situation through location data and detect terrorism activities through data online.

Lastly, some participants found the source of dataveillance vague and intangible. These participants either directly said "I don't know" or could not provide any concrete answer. Instead, they addressed the source of dataveillance as *"they"* throughout the interviews.

Perceived Purposes

The following purposes of dataveillance were identified by the interviewees: *Financial gain, advertising optimization, product development, manipulation,* and *unknown purpose*.

Financial gain was the most salient perceived purpose of dataveillance. Participants either pointed out that "it's just all about making money" (P23) straightforwardly or specified that companies make money through advertising and selling user data. As said by P3, "Companies like Facebook and Google are companies who are running on ads. They need their money from their ads."

Advertising optimization was also frequently mentioned. Participants believed that the data collected were used to make more targeted advertising and generate better ad effects: "They'd like to know about the spending habits of every person. . . . And that is where they can focus their ads on" (P21).

Participants also saw *product development* as a purpose of dataveillance as "sometimes they just need it for the functionality of the app" (P6). Part of the development was also improving the product: "They [Facebook] will probably also use the data to make their platforms better" (P3).

Another perceived dataveillance purpose was *manipulation*. One type of manipulation was to "mold your mind" (P2) by showing content that matched people's interests and changed people over time. Another was to control the public. For example, a few participants pointed out that during the COVID-19 pandemic,

governments could be using people's location data for tracking and managing social distancing practices during the pandemic.

Some participants were *unsure* about the purpose of dataveillance but believed that the data must be used for something. This uncertainty could also coexist with other identified purposes. According to P12, "I think most of it is used for targeted advertisement, but it can't all be targeted advertisement. . . . I'm not sure what actually all this data is used for."

Perceived Mechanisms

Perceived mechanisms are how participants believe the dataveillance practices were conducted. The answers revealed different views on data collection, with one being that data collection was *all-encompassing* and the other being that only *specific data* were collected. Participants also identified the mechanisms of *user profiling* and *data exchange between different parties*. To some, the mechanism remained *unknown*.

Many participants firmly believed that data collection was *all-encompassing*, with a shared consensus that "everything" was collected "all the time." Participants demonstrated this point by either directly saying, "They are just in general collecting everything" (P2) or listing all kinds of data that they believed could be tracked. Moreover, some participants mentioned that data collection was a constant process. For example, P4 believed that her phone was still listening to her conversations even when it was inactive and put in a backpack.

Meanwhile, some were more nuanced and *specific* with the ways data were collected. They believed only certain types of data were collected depending on their experiences, such as browsing history, search history, location, and voice data. They also specified the devices used for collecting data in certain contexts: Mobile phones, laptops, or smart speakers. Some even identified the timing of data collection. For example, P9 said his phone only activated the microphone "when it's unlocked and when the app is being used."

Participants also described *user profiling* as a dataveillance technique in which a profile is built for each user based on both demographic information (e.g., age, gender) and online behavior (e.g., browsing history) to predict the person's interests and preferences: "They just build a huge database of profiling of people" (P3).

Another perceived mechanism was that *different parties exchange the data* they collect about individuals. This could happen among different platforms under the same company, as described by P4: "[Instagram] is owned by Facebook and WhatsApp as well. . . . I think they do share that data." It could also happen between two independent companies, as described by P5: "It might also happen on Google that I'm Google searching for something and then on Facebook it turns up as an ad, or on Instagram. So, I do think that they are also connected." It was also speculated that companies could share data with governments.

Perceived mechanisms were also *unknown*, perhaps even more common than the unknown perceived sources and purposes. This high level of uncertainty was observed not only among participants who directly said, "I don't know" but also among people who provided answers. Participants often stressed that they were unsure about the answers they were giving. Words such as "maybe" and "probably" were frequently used during the conversations about dataveillance mechanisms.

Folk Theories of Dataveillance

When linking the three dimensions (sources, purposes, and mechanisms), we identified three major folk theories of dataveillance. First, *companies do everything to collect data for money*. In this theory, commercial companies, regardless of their size, engage in a variety of activities to collect data from users for financial gains. The activities include collecting either "everything" or specific types of data, exchanging data among different parties, and user profiling, which covered all the mechanisms we identified. Most individuals believed that money was made through advertising and selling user data.

The second folk theory is *technologies collect specific data for companies.* Here, technologies are seen as the tools for companies to achieve their dataveillance goals. Although technologies could be perceived as the direct source of dataveillance, participants did not think technologies have the "intelligence" to conduct dataveillance autonomously. Specific technologies were also more often associated with specific types of data instead of the all-encompassing data collection mechanism.

Third, *governments surveil for manipulation*. This theory was the least personal one as the discussions primarily stemmed from the news or one's speculations. While individuals did not have explicit theories on how governments surveil (i.e., the mechanism), they firmly believed that governments do engage in dataveillance practices for manipulative purposes, such as monitoring epidemics, censorship, and detecting terrorism. Additionally, multiple theories could coexist for each individual.

Positive Thoughts and Feelings

The positive thoughts and feelings could be categorized into three categories: *Better user experience*, *benefits beyond the realm of technology*, and *smartness*.

All participants indicated that they had *better user experiences* thanks to dataveillance. Dataveillance added convenience as it "makes things easier" (P4). Personal relevance was another benefit that dataveillance provided. Participants enjoyed well-made personalized recommendations from platforms like Spotify and YouTube. Personalized advertising was also preferred compared with non-personalized ads because "I'd rather have ads that I have a connection with than ads that I don't have a connection with at all" (P20). Moreover, participants also mentioned that dataveillance made the interaction with technologies more "helpful," "comfortable," and "fun."

A few participants mentioned several *benefits beyond the realm of technology*. P8 noted that Apple Watch collected his movement data and nudged him to exercise more, which improved his health. P18 mentioned that being able to use Siri (who was constantly listening) when driving made him feel safer.

Dataveillance was also perceived to be *smart* because of the advanced technologies and complicated systems being used. Participants were "amazed by how they can do it with the technology" (P6). As said by P5, "It's smart that they thought about it, and that they invented it."

Negative Thoughts and Feelings

Regarding the negative thoughts and feelings, participants mentioned the following: *Imbalanced power, concerns over unethical practices, concerns over personal data, feelings of violation,* and *creepiness*.

A lot of negative thoughts and feelings about dataveillance centered around the *imbalanced power* between the individuals and the source of dataveillance, commercial companies in particular. Participants themselves often perceived a lack of control or a sense of powerlessness regarding the situation: "You can't really do anything about it" (P5). Meanwhile, they considered that companies, especially Big Tech companies such as Google and Facebook, "have too much power by knowing everybody's profile" (P4). On top of that, as highlighted by P11, "they collect data in all areas. . . . They know your social communication, and they know your relationships, and they know also what you're buying or partly they know what you've been buying." These companies were seen as being able to collect numerous types of data from everyone with their technological ecosystems, which aggravated the power imbalance.

Another salient category was *concerns over unethical practices*. Participants complained that companies used covert persuasion strategies to make people stay longer on their platforms, hid advertisements among social feeds, and "seduced" people to give apps access to their cameras and microphones because only then they could use certain functions. Moreover, some companies were criticized for providing misleading messages: "The big companies will never say that they are actually spying on all people. . . . They are saying that they don't, but they do" (P16). Unethical practices also included threats to personal freedom. P5 used the social credit system in China as an example, but this threat was not limited to government dataveillance. P12, for instance, felt limited freedom in general when using technologies: "I want to just be able to do whatever I want to do without having to think about that what I'm doing is actually being recorded."

Concerns over personal data as another category included both privacy concerns and data security concerns. Privacy concerns were about media technologies collecting too much and too private data from individuals: "They take a lot of data from you" (P17). Data security concerns stemmed from worries that the collected data might be hacked and acquired by third parties illegally: "What if it gets hacked, or if it gets leaked, or if there happens to be someone at Apple who doesn't have such good intentions?" (P23).

Emotionally, participants felt a sense of *violation* because they thought the dataveillance sources had crossed the boundaries people had in their minds by collecting personal data that were too sensitive and using these for inappropriate purposes such as manipulating the public's political views. As said by P9, "That's too far. That crosses the line."

Dataveillance was also perceived to be *creepy* and *scary*, signaling people's unsettling fear, which came from realizing that companies knew too much about themselves. P3 mentioned Google knew he was catching a flight; P6 noticed that Google could accurately autocomplete his searches; P8 received a LinkedIn

suggestion to connect with a new colleague from whom he had just gotten the phone number. Like P5 said, "It's kind of creepy that they know everything about you."

Coping Strategies

Other than the positive and negative evaluations, participants very often gave unprompted rationalizations of why they chose to continue using media technologies despite knowing they were under dataveillance. Following the literature on privacy cynicism (Hoffmann, Lutz, & Ranzini, 2016) and persuasive communication (Eisend & Tarrahi, 2022; Friestad & Wright, 1994), the thought processes that described participants' cognitive efforts to deal with and rationalize their media technology use under dataveillance were labeled in this study as cognitive coping strategies. They included the seemingly conflicting notions of *lacking agency to avoid dataveillance (resigning)* and *having sufficient agency under dataveillance (self-empowering)* as well as *downplaying the cost of dataveillance* and *sympathizing with commercial companies*.

Resigning

Many participants tried to rationalize their conflicted thoughts, feelings, and behavior with their *lack of agency to avoid dataveillance*, meaning that they were unable to change the situation. People who adopted this coping strategy believed that dataveillance was unavoidable because "everywhere your privacy is violated" (P7) and normalized dataveillance as a "common practice" (P16). Meanwhile, they heavily relied on the services that these technologies provided: "You can't live without them" (P21). Multiple participants used the phrase "it is what it is" to describe this situation, implying their perceived inability and reluctance to change the situation.

Self-Empowering

Contrarily, some people argued that they did *have sufficient agency under dataveillance* and had control over the situation despite dataveillance. A common rationale was that everyone was responsible for their own choice: "It's something you choose to do when you use their products, and I am aware of it and I am annoyed by it, but I still choose to use it" (P9). They also argued that people always had the choice of not using dataveillance-enabling technologies: "If you don't want to, you don't have to. You don't have to use a smartphone" (P2). Some participants also mentioned that they believed they could protect themselves by adjusting privacy settings, using privacy protection software, or limiting the data shared online.

Downplaying

Another way of coping was to *downplay the cost of dataveillance*. People argued that their data were not important or not valuable to the dataveillance sources. As P1 said, "What kind of use is it to them anyways? It's not like you're going anywhere interesting." Another reason was that the data being collected were not personal enough to do any harm: "What harm is there that they know that I still like potatoes?" (P11). Another phrase that was used frequently by the participants was "I have nothing to hide" as they were not engaging in any illegal or embarrassing activities.

Sympathizing

Lastly, several participants expressed their *sympathy for dataveillance sources*, mostly commercial companies. They put themselves in the perspectives of the dataveillance sources and understood that companies also needed to make profits, especially when a lot of digital services were provided for free. As P1 said, "I would do that as well." One participant also showed sympathy for governments that needed dataveillance to ensure national security or manage the pandemic situation: "It's not that they [the government] intentionally want to control their people, let's be honest. They want to do the best for public health. They want to work on society without terrorists or to prevent it" (P11).

Connecting Thoughts, Feelings, and Folk Theories

Similar to folk theories, multiple positive and negative thoughts and feelings as well as coping strategies were often observed within each individual simultaneously. In fact, participants likely developed the coping strategies due to their conflicting and coexisting thoughts and feelings. Some were more mindful about having both positive and negative evaluations and explicitly mentioned the cost-benefit tradeoff: "You're kind of giving away certain privacy for some comfort, I guess" (P9).

Importantly, we found that whether participants felt positive or negative about a dataveillance episode often depended on the perceived mechanism dimensions in their folk theories, specifically, the types of data that they thought were being collected. Participants generally did not mind too much when the data being collected were shopping history, browsing history, or social media behavior. However, they were more likely to have negative thoughts and feelings when they perceived the collected data as sensitive data, such as political views, banking information, location, and real-life conversations.

Furthermore, those who had more uncertainty in their folk theories (i.e., answered with an unknown source/purpose/mechanism) used the resigning strategy much more than the others. Contrarily, people who gave detailed folk theories on each dimension were the most likely to use the self-empowering strategy.

Discussion

The current study had two aims: Delineating the folk theories of dataveillance through the dimensions of perceived sources, purposes, and mechanisms, and exploring people's thoughts and feelings about dataveillance. The results make several contributions to our knowledge about dataveillance in media technologies.

The first main finding pertains to the three major folk theories of dataveillance: *Companies do everything to collect data for money*; *technologies collect specific data for companies*; and *governments surveil for manipulation*, all of which show that individuals' beliefs resonate with the scholarly discussions of dataveillance. The first folk theory identifies the commodification of personal data in exchange for financial gains, which corresponds with the notion of surveillance capitalism (Zuboff, 2019). This demonstrates that people are knowledgeable about the underlying purpose of corporate dataveillance. The second theory suggests that while technologies can be seen as the sources of communication (Guzman, 2019), people do not perceive them as

the sources of dataveillance since the act of dataveillance requires a higher level of autonomy and consciousness. The third folk theory shows that individuals are aware of state dataveillance (Lyon, 2014; Marx, 2015), yet do not see its impact as prominent as that of corporate dataveillance in their daily lives. There is also more uncertainty about the purposes of state dataveillance, which is in contrast with people's adamancy in the capitalistic purpose of corporates. As one of the few studies that gathered folk theories of dataveillance across unconstrained realms, this finding illustrates that in individuals' minds, dataveillance is not just the act of one (type of) entity but a collection of everyday forms of monitoring. Our participants conceptualize dataveillance as being conducted by various sources and for various purposes, indicating the omnipresence of dataveillance in people's beliefs. Moreover, as both corporate and state dataveillance appear in the same dialogue, we are able to compare them and conclude that corporate dataveillance takes a much more prominent position in shaping people's perceptions of feeling surveilled than state surveillance.

The second key finding concerns the widespread *uncertainty* in the folk theories, particularly regarding perceived mechanisms. Although individuals hold relatively strong beliefs regarding the sources and purposes of dataveillance, they struggle to provide concrete explanations for how they are being surveilled. Uncertainty is high among participants, including those with relatively high technological literacy. This uncertainty indicates a low level of awareness of dataveillance mechanisms due to information and power asymmetry between the dataveillance sources and subjects (Andrejevic, 2014; Lyon, 2009; Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016). According to the transparency-awareness-control framework (Segijn, Strycharz, Riegelman, & Hennesy, 2021), without a sufficient level of awareness, users cannot assert control over the extent to which they are surveilled. Furthermore, this finding informs literacy programs that only educating individuals about the sources and purposes of dataveillance may not suffice. People's feelings of powerlessness and concerns stem from their uncertainty regarding the mechanisms of dataveillance. Future interventions should place more emphasis on explaining how exactly data are collected, shared, and used so that people feel adequately informed. Additionally, our participants have criticized the transparency features of technological platforms such as privacy policies and cookie messages being lengthy and vague, which directly contribute to the uncertainties in this dimension. Corporates should take responsibility and present relevant information in a precise and concise manner.

Third, some individuals also hold false beliefs about dataveillance mechanisms, such as phones eavesdropping on their conversations (Tidy, 2019). In such cases, since individuals believe that real-life conversations are used for dataveillance and perceive this practice as collecting highly sensitive data, they develop a more negative view of dataveillance. This finding supports the argument that folk theories can significantly impact one's dataveillance beliefs and subsequent responses, regardless of the accuracy of the theories (Strycharz & Segijn, 2022). It is also speculated that people who tend to hold such false beliefs may exhibit the trait of conspiracy mentality—the tendency to believe in conspiracy theories (Bruder, Haffke, Neave, Nouripanah, & Imhoff, 2013). Zhang and colleagues (2023) found that individuals with a conspiracy mentality are more likely to experience heightened feelings of surveillance. Our finding could offer an explanation for this relationship, which is that people with a conspiracy mentality might base their folk theories on inaccurate information, leading to an unjust evaluation of dataveillance. Future research could explore the extent to which misinformation, disinformation, or conspiracy theories influence the development of folk theories and people's responses to dataveillance.

Fourth, our study reveals that individuals believe that dataveillance improves their user experiences, brings benefits beyond the realm of technology, and is smart. Meanwhile, they perceive an imbalanced power, have concerns over unethical practices and their data, feel violated, and find dataveillance creepy. This is in line with the privacy calculus that costs and benefits coexist (Dinev & Hart, 2006) and has been referred to as the personalization(-privacy) paradox (Boerman & Smit, 2023).

More importantly, on a closer examination of the costs and benefits, perceived benefits appear to be *more personal*, *realistic*, *and immediate* than the costs. Most benefits of dataveillance relate to better user experiences, which are rewarded instantly to individuals with each user interaction. Contrarily, the costs—imbalanced power, ethical concerns, and data concerns—do not necessarily impact the individuals themselves and often seem hypothetical. While these remain valid concerns, they do appear to be less personal, less realistic, and more distant. Given the potentially different weights of benefits and costs, we theorize that the benefits may play a more critical role in people's decision making, which makes the option of continued disclosure of personal information more attractive. However, further research is needed to quantify the weights people assign to different benefits and costs in the privacy calculus to assess whether individuals indeed prioritize benefits due to their personal relevance, psychological closeness, and perceived immediacy.

Going beyond the privacy calculus, our last key finding is a typology of cognitive coping strategies that people employ to rationalize their use of media technologies when having mixed thoughts and feelings about dataveillance, including *resigning*, *self-empowering*, *downplaying*, and *sympathizing*. The first coping strategy *resigning* corroborates with the concepts of digital resignation (Draper & Turow, 2019) and privacy cynicism (Hoffmann et al., 2016), both of which describe the feeling of frustration, powerlessness, and futility in engaging in any privacy protection behavior. *Downplaying* shares synergies with the "nothing to hide" rhetoric found in Marwick and Hargittai (2019, p. 1708). Furthermore, there are also individuals who perceive sufficient agency under dataveillance (*self-empowering*) and reaffirm themselves with arguments that support their current attitude and behavior. This strategy resonates with attitude bolstering, a commonly used strategy by individuals to resist persuasion (Jacks & Cameron, 2003). The final coping strategy is *sympathizing* with the dataveillance sources, meaning that individuals take the perspective of the dataveillance source to understand why certain dataveillance practices are employed. People who adopt different coping strategies seem to vary in their levels of certainty regarding their folk theories. Participants with more concrete theories tended to engage in self-empowerment, while those who showed less certainty in their theories almost unanimously resorted to the resigning strategy. This underscores the crucial role of certainty in shaping one's agency to cope with dataveillance. Furthermore, the adoption of different coping strategies also seems to relate to individuals' cost-benefit evaluations and privacy protection behavior. Future research could validate this typology, identify the distinct traits of each coping type, and quantitatively examine the relationship between individuals' coping types and their dataveillance perceptions and responses (a similar approach to Voorveld, Meppelink, & Boerman, 2023). From a practical perspective, the diverse coping strategies identified in this study suggest varying needs in intervention strategies. For instance, individuals employing the resigning strategy might appreciate interventions aimed at increasing agency and mitigating privacy cynicism, while people using the downplaying strategy could benefit from interventions that raise awareness of privacy threats. However, it is crucial to acknowledge that previous efforts to address these needs have faced significant challenges (e.g., Boerman, Strycharz, & Smit, 2024), underscoring the obscurity of finding effective interventions. Nonetheless, our study offers a more nuanced

understanding of dataveillance coping strategies and their implications for intervention. Our typology of coping strategies can serve as an entry point to identify different needs and implement tailored interventions for various groups.

References

Andrejevic, M. (2014). Big data, big questions| The big data divide. *International Journal of Communication, 8*, 1673–1689.

Bakir, V., Cable, J., Dencik, L., Hintz, A., & McStay, A. (2015, November). *Public feeling on privacy, security and surveillance: A report by DATA-PSST and DCSS*. Retrieved from https://dcssproject.net/public-feeling/

Boerman, S. C., & Smit, E. G. (2023). Advertising and privacy: An overview of past research and a research agenda. *International Journal of Advertising, 42*(1), 60–68. doi:10.1080/02650487.2022.2122251

Boerman, S. C., Strycharz, J., & Smit, E. G. (2024). How can we increase privacy protection behavior? A longitudinal experiment testing three intervention strategies. *Communication Research, 51*(2), 115–145. doi:10.1177/00936502231177786

Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. Los Angeles, CA: SAGE.

Bruder, M., Haffke, P., Neave, N., Nouripanah, N., & Imhoff, R. (2013). Measuring individual differences in generic beliefs in conspiracy theories across cultures: Conspiracy mentality questionnaire. *Frontiers in Psychology, 4*, 1–15. doi:10.3389/fpsyg.2013.00225

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society, 20*(1), 30–44. doi: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. doi: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. doi:10.1080/1369118X.2021.1989011

Carver, L. F., & Mackinnon, D. (2020). Health applications of gerontechnology, privacy, and surveillance: A scoping review. *Surveillance & Society, 18*(2), 216–230. doi:10.24908/ss.v18i2.13240

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). London, UK: SAGE.

Christin, A. (2020). What data can do: A typology of mechanisms. *International Journal of Communication, 14*, 1115–1134.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498–512. doi:10.1145/42411.42413

Dencik, L., & Cable, J. (2017). Digital citizenship and surveillance| The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11*, 763–781.

DeVito, M. A., Birnholtz, J., Hancock, J. T., French, M., & Liu, S. (2018). How people form folk theories of social media feeds and what it means for how we study self-presentation. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). Montreal, QC: Association for Computing Machinery. doi:10.1145/3173574.3173694

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: Association for Computing Machinery. doi:10.1145/3025453.3025659

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. doi:10.1287/isre.1060.0080

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824–1839. doi:10.1177/1461444819833331

Duffy, B. E., & Chan, N. K. (2019). "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society, 21*(1), 119–138. doi:10.1177/1461444818791318

Eisend, M., & Tarrahi, F. (2022). Persuasion knowledge in the marketplace: A meta-analysis. *Journal of Consumer Psychology, 32*(1), 3–22. doi:10.1002/jcpy.1258

Fowler, B. (2019, July 10). *Is your smartphone secretly listening to you?* Consumer Reports. Retrieved from https://www.consumerreports.org/smartphones/is-your-smartphone-secretly-listening-to-you/

Friestad, M., & Wright, P. (1994). The persuasion knowledge model: How people cope with persuasion attempts. *Journal of Consumer Research, 21*(1), 1–31. doi:10.1086/209380

Fuchs, C. (2011). New media, Web 2.0 and surveillance. *Sociology Compass, 5*(2), 134–147. doi:10.1111/j.1751-9020.2010.00354.x

Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden. *Journal of Information, Communication and Ethics in Society, 15*(4), 412–444. doi:10.1108/JICES-01-2016-0004

Gelman, S. A., & Legare, C. H. (2011). Concepts and folk theories. *Annual Review of Anthropology, 40*(1), 379–398. doi:10.1146/annurev-anthro-081309-145822

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, IL: Aldine Publishing.

Guzman, A. L. (2019). Voices in and of the machine: Source orientation toward mobile virtual assistants. *Computers in Human Behavior, 90*, 343–350. doi:10.1016/j.chb.2018.08.009

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), Article 7. doi:10.5817/CP2016-4-7

Huang, S. A., Hancock, J., & Tong, S. T. (2022). Folk theories of online dating: Exploring people's beliefs about the online dating process and online dating algorithms. *Social Media + Society, 8*(2), 1–12. doi:10.1177/20563051221089561

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication, 61*(4), 575–595. doi:10.1111/j.1460-2466.2011.01570.x

Jacks, J. Z., & Cameron, K. A. (2003). Strategies for resisting persuasion. *Basic and Applied Social Psychology, 25*(2), 145–161. doi:10.1207/S15324834BASP2502_5

Jung, A.-R. (2017). The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. *Computers in Human Behavior, 70*, 303–309. doi:10.1016/j.chb.2017.01.008

Kalmus, V., Bolin, G., & Figueiras, R. (2022). Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. *New Media & Society*. Advance online publication, 1–23. doi:10.1177/14614448221134493

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. doi:10.1016/j.ijhcs.2023.103120

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635. doi:10.1111/isj.12062

Kim, H., & Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising, 38*(1), 92–105. doi:10.1080/10641734.2016.1233157

Kristensen, D. B., & Ruckenstein, M. (2018). Co-evolving with self-tracking technologies. *New Media & Society, 20*(10), 3624–3640. doi:10.1177/1461444818755650

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction, 2*(CSCW), 1–31. doi:10.1145/3274371

Lupton, D., & Michael, M. (2017). "Depends on who's got the data": Public understandings of personal digital dataveillance. *Surveillance & Society, 15*(2), 254–268. doi:10.24908/ss.v15i2.6332

Lyon, D. (2009). Surveillance, power, and everyday life. In C. Avgerou, R. Mansell, D. Quah, & R. Silverstone (Eds.), *The Oxford handbook of information and communication technologies* (1st ed., pp. 449–468). Oxford, UK: Oxford University Press. doi:10.1093/oxfordhb/9780199548798.003.0019

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society, 1*(2), 1–13. doi:10.1177/2053951714541861

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society, 22*(12), 1697–1713. doi:10.1080/1369118X.2018.1450432

Marx, G. T. (2015). Surveillance studies. In J. D. Wright (Ed.), *International encyclopedia of the social & behavioral sciences* (2nd ed., pp. 733–741). Oxford, UK: Elsevier. doi:10.1016/B978-0-08-097086-8.64025-4

McEwan, B., & Flood, M. (2018). Passwords for jobs: Compression of identity in reaction to perceived organizational control via social media surveillance. *New Media & Society, 20*(5), 1715–1734. doi:10.1177/1461444817706073

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21. doi:10.1177/2053951716679679

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: SAGE.

Phelan, C., Lampe, C., & Resnick, P. (2016). It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 5240–5251). San Jose, CA: Association for Computing Machinery. doi:10.1145/2858036.2858381

Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy, 13*(1), 12–24. doi:10.1080/17530350.2019.1574866

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. doi:10.17645/mac.v9i4.4054

Siles, I., Segura-Castillo, A., Solís, R., & Sancho, M. (2020). Folk theories of algorithmic recommendations on Spotify: Enacting data assemblages in the global South. *Big Data & Society, 7*(1), 1–15. doi:10.1177/2053951720923377

Smit, E. G., van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior, 32*, 15–22. doi:10.1016/j.chb.2013.11.008

Squires, A. (2009). Methodological challenges in cross-language qualitative research: A research review. *International Journal of Nursing Studies, 46*(2), 277–287. doi:10.1016/j.ijnurstu.2008.08.006

Stanton, J. M., & Stam, K. R. (2003). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance & Society, 1*(2), 152–190. doi:10.24908/ss.v1i2.3351

Strycharz, J., & Segijn, C. M. (2022). The future of dataveillance in advertising theory and practice. *Journal of Advertising, 51*(5), 574–591. doi:10.1080/00913367.2022.2109781

Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019). Consumer view on personalized advertising: Overview of self-reported benefits and concerns. In E. Bigne & S. Rosengren (Eds.), *Advances in advertising research X: Multiple touchpoints in brand communication* (pp. 53–66). Wiesbaden, Germany: Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-24878-9_5

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review, 8*(2), 1–22. doi:10.14763/2019.2.1410

Tidy, J. (2019, September 5). Why phones that secretly listen to us are a myth. *BBC News*. Retrieved from https://www.bbc.com/news/technology-49585682

Turow, J. (2021). *The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet*. New Haven, CT: Yale University Press.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (pp. 1–15). New York, NY: Association for Computing Machinery. doi:10.1145/2335356.2335362

van Deursen, A. J. A. M., Helsper, E. J., & Eynon, R. (2016). Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society, 19*(6), 804–823. doi:10.1080/1369118X.2015.1078834

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208. doi:10.24908/ss.v12i2.4776

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). "Okay google, what about my privacy?": User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior, 120*, 106763. doi:10.1016/j.chb.2021.106763

Voorveld, H. A. M., Meppelink, C. S., & Boerman, S. C. (2023). Consumers' persuasion knowledge of algorithms in social media advertising: Identifying consumer groups based on awareness, appropriateness, and coping ability. *International Journal of Advertising.* Advance online publication, 1–27. doi:10.1080/02650487.2023.2264045

Voorveld, H. A. M., Segijn, C. M., Ketelaar, P. E., & Smit, E. G. (2014). Investigating the prevalence and predictors of media multitasking across countries. *International Journal of Communication, 8*, 2755–2777.

Ytre-Arne, B., & Moe, H. (2021). Folk theories of algorithms: Understanding digital irritation. *Media, Culture & Society, 43*(5), 807–824. doi: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, Germany: Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-40429-1_12

Zhao, L. (2023). Filter bubbles? Also protector bubbles! Folk theories of Zhihu algorithms among Chinese gay men. *Social Media + Society, 9*(2), 1–10. doi:10.1177/20563051231168647

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (1st ed.). New York, NY: PublicAffairs.