Feeling watched

Understanding triggers of and responses to perceived surveillance in digital technologies

Zhang, D.

Publication date
2026

CHAPTER 6

GENERAL DISCUSSION AND CONCLUSION

This dissertation investigated the phenomenon of perceived surveillance—people's feeling of being watched, listened to, or having their personal data recorded—in a digital landscape where dataveillance is becoming increasingly pervasive. It aimed to address four specific research gaps. First, it mapped individuals' beliefs about dataveillance, including conceptualizations of and evaluations about dataveillance. Second, it examined the specific triggers of perceived surveillance, namely perceived and objective accuracy of algorithmic profiling and the sensitivity and amount of data used in digital data-driven advertising. Third, it investigated the consequences of perceived surveillance in terms of how people cope with dataveillance as well as how people respond to data-driven advertising. Fourth, it explored the individual differences and contextual factors that are related to perceived surveillance.

Based on a multi-methodological approach combining in-depth interviews, surveys, and an experiment, this final chapter presents six key findings and their theoretical implications. It then discusses the practical implications, limitations, future research directions, and implications for individual digital technology users.

KEY FINDINGS

Key finding 1: Data-driven advertising shapes the main folk theory—*Companies do everything to collect data for money*

This dissertation revealed a variety of conceptualizations of dataveillance by individuals. These conceptualizations are built upon the dimensions of perceived source, purpose, and mechanisms. Together, they form the folk theories of dataveillance, which are intuitive and informal theories based on individuals' personal experiences that explain the workings of technological systems (DeVito et al., 2017; Gelman & Legare, 2011). Through in-depth interviews, Chapter 2 identified three major folk theories that people hold about dataveillance. The first and most prominent theory is that *companies do everything to collect data for money*. The second one is that *technologies collect specific data for companies*. And the third and least prominent one is that *governments surveil for manipulation*. Chapter 3 provided quantitative, representative findings within the Dutch population that showed the same pattern, where commercial actors, including advertisers, companies in general, and social media platforms, are perceived as sources of dataveillance by most individuals. In comparison, AI, devices, and government are perceived as less prominent sources. While Chapter 2 mainly identified financial gains and manipulation as the corresponding purposes of companies and governments, Chapter 3 compared several more detailed commercial purposes (e.g., advertising, personalized content, sell to others, tracking, product improvement, etc.) and identified advertising as

the main perceived purpose of dataveillance. This shows that data-driven advertising plays a key role in shaping the most prominent folk theory, *companies do everything to collect data for money*.

One theoretical contribution of this finding lies in highlighting the prominence of corporate surveillance while also providing a holistic view of how different forms of dataveillance shape individuals' folk theories. Although both corporate surveillance and state surveillance have been extensively discussed by academic scholars (Marx, 2015) and are now taking place on the same technological platforms (Kalmus et al., 2022), previous research has not yet examined their prominence from individuals' perspectives. Our finding offers important insights on this: To individuals, corporate surveillance is way more prominent in their daily digital experiences than state surveillance. Individuals' beliefs that companies commodify personal data in exchange for financial gains are highly in line with the notion of surveillance capitalism (Zuboff, 2019), indicating their awareness toward the underlying goals of corporate dataveillance.

Furthermore, the identification of advertisers as the main source and advertising as the main purpose of dataveillance suggests that individuals' awareness of companies profiting through data-driven advertising substantially contributes to the formation of the first folk theory. Therefore, data-driven advertising is also a key driver in shaping people's beliefs about dataveillance. This indicates that data-driven advertising constitutes a large proportion of individuals' dataveillance experiences and therefore triggers the most perceived surveillance among individuals, validating earlier studies on perceived surveillance that focused on this context (Farman et al., 2020; Segijn, Kim, & van Ooijen, 2024; Sifaoui & Segijn, 2025).

Moreover, individuals perceive technologies as direct sources of dataveillance but also believe that they are ultimately controlled by companies. Having the belief that algorithms, phones, or web browsers are surveilling them could be the result of technologies being perceived as communicators, the key proposition within human-machine communication (Guzman & Lewis, 2020). However, individuals do not deem the technologies to have enough autonomy or consciousness to be initiators of dataveillance. They feel surveilled by technologies, but they know that technologies are employed by companies. This finding offers a nuanced understanding regarding the role of technologies in dataveillance practices.

Key finding 2: People see both benefits and costs of dataveillance

Having formed a conceptualization of dataveillance, people develop mixed thoughts and feelings about dataveillance. On the one hand, dataveillance improves user experience, brings benefits beyond the realm of technology (e.g., health benefits), and is considered

as "smart." On the other hand, people perceive the power imbalance between dataveillance sources and themselves, have concerns over unethical practices and privacy, and emotionally feel violated and find it creepy.

This finding theoretically contributes to our understanding of privacy calculus by incorporating the affective dimension in the cost-benefit assessment, identifying feelings of violation and creepiness as perceived costs of dataveillance. Privacy calculus originally describes a rational process, but recent research has proposed and examined irrational factors influencing privacy calculus, such as emotions (Fernandes & Pereira, 2021; Kehr et al., 2015; Plangger & Montecchi, 2020). This finding extends this body of knowledge, and maps out affective elements that add to the perceived costs in the calculus.

A closer examination of the perceived benefits and costs also revealed that the benefits seem to be more personal, realistic, and immediate than the costs. Benefits like better user experience or health benefits are actually experienced by individuals when they use the technologies, while costs like power imbalances, ethical issues, and data concerns are typically more abstract, less personal, and may not directly affect individuals, making them far less tangible and more distant. As suggested by Dinev and Hart (2006), beliefs can carry different weights such that one strong belief can outweigh the influence of the others. Due to psychological distortions, individuals tend to choose immediate gratifications and discount long-term risks when making privacy decisions (Acquisti, 2004). The perceived benefits might weigh more in the calculus than the costs precisely because they are more personal, realistic, and immediate. This might provide an explanation to why people are still engaged with digital technologies despite being under dataveillance, expanding our current knowledge on individuals' privacy decision-making.

Key finding 3: Accuracy of algorithmic profiling and sensitivity and amount of data used in data-driven advertising influence perceived surveillance

Perceived surveillance is triggered when people observe instances of data collection episodes (e.g., viewing one's algorithmic profile, or seeing data-driven ads on social media). These are called surveillance episodes (Strycharz & Segijn, 2022). Yet, specific features of a surveillance episode can influence the level of perceived surveillance to different degrees. The third key finding of the dissertation is that perceived and objective accuracy of algorithmic profiling, as well as the sensitivity and amount of data used in data-driven advertising, influence the extent to which individuals feel surveilled after being exposed to the surveillance episode.

First, both perceived and objective accuracy of algorithmic profiling are positively related to the level of perceived surveillance. In Chapter 4, we asked participants to view their own

personal algorithmic profiles on Google My Ad Center (Google, n.d.-c). These profiles depicted inferences about one's sociodemographic categories and interests predicted by Google. We measured the perceived and objective accuracy of algorithmic profiling, which were respectively the subjective and objective evaluations of how much the profiles reflected themselves as individuals. We found that the more objectively accurate one's algorithmic profile is, and the more accurate one perceives their algorithmic profile to be, the more they feel surveilled.

Second, using highly sensitive data (e.g., income level, current location) or multiple types of data in data-driven advertising evokes higher perceived surveillance than using less sensitive data (e.g., gender, age) or a single type of data. There is also an interaction effect between data sensitivity and data amount. Data-driven advertising using high-sensitivity data always leads to higher perceived surveillance compared to advertising that uses low-sensitivity data, regardless of the amount of data being used. However, using multiple types of data does not lead to higher perceived surveillance than using a single type of data when the data sensitivity is high. This suggests that data sensitivity plays a more influential role than data amount in shaping perceived surveillance.

This finding provides an important theoretical contribution to the DEAL framework as to how and why perceived surveillance is triggered (Strycharz & Segijn, 2022). Although the DEAL framework suggests that encountering surveillance episodes leads to perceived surveillance, it does not clarify or explain how the characteristics of the data or the outcome of data collection may result in differing degrees of perceived surveillance (Strycharz & Segijn, 2022). This dissertation proposes and explains this proposition using psychological ownership theory (Pierce et al., 2003) and communication privacy management theory (Petronio, 2002). In situations where people directly observe the collection of data (e.g., through transparency features disclosing the data used in the advertisement), the sensitivity and amount of data can determine how strictly the privacy boundaries are managed and therefore determine the likelihood of one's privacy boundaries being intruded. Boundary intrusion, or boundary turbulence, occurs when individuals become aware that companies who are not supposed to know certain personal information do have knowledge of the information (Petronio, 2002). How strictly the boundaries are managed and how much they are intruded can affect the level of perceived surveillance being triggered. In situations where users only indirectly observe the outcomes of dataveillance (e.g., seeing algorithmic inferences made about oneself), these outcomes of data collection may feel close or distant to oneself depending on how accurately the information describe themselves. People might then feel more or less ownership toward these outcomes of data collection (van Dijk & van Knippenberg, 2005). By integrating these theories, we extend the DEAL framework to account for and explain how specific features of surveillance episodes may elicit perceived surveillance to

different degrees. This finding shows that the characteristics of the data used (i.e., sensitivity and amount of data) and how they are used (i.e., making accurate or inaccurate inferences) within a surveillance episode influence the extent to which perceived surveillance is triggered, providing valuable empirical evidence that is currently lacking in the literature.

Key finding 4: People cope with perceived surveillance by having stronger privacy protection intention but potentially also higher privacy cynicism

As for the consequences of feeling surveilled, Chapter 2 identified four coping strategies that individuals use to rationalize their continued use of digital technologies despite feeling surveilled: privacy cynicism, self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation. Chapter 4 quantitatively examined the relationships between perceived surveillance and these coping strategies as well as privacy protection intention as an additional strategy. We found that the more individuals feel surveilled, the more they intend to adjust their ad settings to limit dataveillance, but they are also more likely to feel that privacy protection is futile (privacy cynicism). However, Chapter 5 paints a different picture of the relationship between perceived surveillance and privacy cynicism, as it did not find any significant effect of perceived surveillance on privacy cynicism. This might be due to the use of different surveillance episodes in these studies. In Chapter 4, individuals viewed their actual algorithmic profiles from Google, while in Chapter 5 participants were exposed to fictitious ads that claimed to use one's personal data. While both situations triggered the feeling of surveillance, the former likely had a stronger real-world implication than the latter. Therefore, they were more likely to develop a more cynical attitude and feel that privacy protection (in real life) is futile. This indicates that privacy cynicism is rather stable and might only change when perceived surveillance is elicited by impactful personal experiences.

While Chapter 2 qualitatively identified more coping strategies than privacy cynicism, namely downplaying dataveillance cost, self-empowerment and sympathizing with the corporation, Chapter 4 found that these coping strategies did not positively relate to perceived surveillance, and there was even a negative relationship between perceived surveillance and downplay dataveillance cost. Instead, we found direct, positive relationships between perceived accuracy of algorithmic profiling and these three coping strategies. This suggests that there might be other mechanisms than perceived surveillance that can explain why people engage in self-empowerment, downplaying, and sympathizing after viewing their accurate algorithmic profiles, such as trust and surprise (Büchi et al., 2023; X. Chen et al., 2022). Nonetheless, the finding shows that they are indeed distinct coping strategies that individuals might adopt for different reasons.

This finding theoretically contributes to our current knowledge of surveillance responses by revealing and examining the coping strategies individuals adopt in response to perceived surveillance. Previous research has predominantly studied the consequences of perceived surveillance through the angle of advertising effectiveness (Segijn et al., 2023; Segijn, Kim, Lee, et al., 2024; Segijn, Kim, & van Ooijen, 2024; Sifaoui & Segijn, 2025). A more limited body of work has explored its behavioral implications, including chilling effects on media behavior and information disclosure behavior (Kappeler et al., 2023; J. Kim et al., 2025; Strycharz & Segijn, 2024). However, there has been little research on how individuals cognitively manage the tension between awareness of dataveillance and continued engagement with digital technologies. This dissertation addresses this gap by showing that other than behavioral responses, individuals also adopt cognitive coping strategies to rationalize why they still use these technologies despite being subjected to dataveillance. These coping strategies are different ways users navigate discomfort without disengagement. By focusing on the cognitive coping strategies rather than just behaviors, this dissertation highlights the psychological outcomes that could potentially hinder individuals' engagement with privacy protection behavior and further limit user agency and exacerbate power imbalances (Draper et al., 2024).

These strategies and how they are influenced by perceived surveillance are grounded in broader theories such as privacy cynicism, digital resignation, persuasion resistance, and reactance theory, but are uniquely contextualized within the realm of dataveillance (Brehm & Brehm, 1981; Draper & Turow, 2019; Fransen et al., 2015; Hoffmann et al., 2016). Our finding adds to the knowledge about privacy cynicism by showing that perceived surveillance can be an antecedent to it when it is triggered by impactful personal experiences. It also contributes to the persuasion resistance literature by showing that several established resistance strategies (i.e., avoidance, inertia, empowerment, biased processing, and source contesting; Fransen et al., 2015) can manifest in the forms of privacy protection behavior, privacy cynicism, self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation. By doing so, we bring the classic resistance strategies into a new digital dataveillance context.

Key finding 5: Perceived surveillance damages attitudes toward the ad, brand, and platform

Perceived surveillance also impacts how people respond to data-driven advertising. Chapter 5 found that perceived surveillance damages the attitude toward the ad, brand, as well as the platform. Platforms are channels through which the ad is displayed, such as a social media platform or a third-party website. When individuals are exposed to data-driven advertisements that trigger their feeling of being surveilled, they develop more

negative attitudes not only toward the ad and brand, but also the platform displaying the ad.

This finding expands the literature on the effects of perceived surveillance on advertising responses by revealing its negative impact on individuals' evaluations of platforms. While previous research has focused on how perceived surveillance influences individuals' evaluations of the ad and brand (Segijn et al., 2023; Segijn, Kim, Lee, et al., 2024; Segijn, Kim, & van Ooijen, 2024; Sifaoui & Segijn, 2025), less attention has been given to its impact on evaluations of the platform. Chapter 2 and 3 suggest that both advertisers and social media platforms are perceived as sources of dataveillance, yet there is limited empirical evidence on how this might affect platform evaluations. This finding provides novel insight, showing that any party that is (perceived to be) involved in the dataveillance practice can be evaluated more negatively when individuals encounter persuasive messages based on their personal data. This also extends the DEAL framework by adding another outcome of perceived surveillance next to ad and brand responses.

Furthermore, this finding adds to our understanding of how individuals see the role of platforms in dataveillance. Although platforms tend to position themselves as neutral channels (van Dijck et al., 2018), the finding suggests that individuals do not see them as neutral. Instead, when individuals feel surveilled due to seeing data-driven ads, they extend the negative evaluations to both the brand and the platform. This indicates that people do hold platforms accountable for the dataveillance practices that enable data-driven advertising.

Key finding 6: Perceived surveillance varies with individual differences and technological contexts

The last key finding is that perceived surveillance is related to both individual differences and technological contexts. Specifically, demographic characteristics like age and education, and psychological factors including privacy concerns, online privacy literacy, and conspiracy mentality are associated with the level of perceived surveillance. Regarding technological contexts, social media and web browsers are contexts in which individuals feel the most surveilled.

Chapter 3 revealed that perceived surveillance is related to a number of individual characteristics. Privacy concerns and conspiracy mentality are both positively associated with perceived surveillance, while technology trust is not related to perceived surveillance. Younger adults tend to perceive higher levels of surveillance than older adults. Highly educated individuals tend to have higher levels of perceived surveillance than those with lower education levels. Gender does not play a significant role. Chapter 4 investigated the moderating role of online privacy literacy on the relationships between perceived

surveillance and coping strategies, where we found that online privacy literacy moderates the relationship between perceived surveillance and privacy cynicism.

Furthermore, Chapter 3 found that the technological context also plays a role in how much people feel surveilled. Individuals tend to view social media as the most surveilling platform, with web browsers also standing out as particularly surveilling in comparison to other technologies. Navigation apps and virtual assistants are perceived similarly and slightly surveilling. People are rather ambivalent about smartphones and smart speakers. In contrast, smart watches and smart home devices were perceived as not surveilling overall.

This finding makes a significant theoretical contribution by empirically supporting the proposition of the DEAL framework that both individual differences and contextual factors shape responses to dataveillance (Strycharz & Segijn, 2022). While prior research has tapped into the roles of a few individual traits in perceptions of dataveillance (e.g., Kalmus et al., 2022; Segijn & van Ooijen, 2020), this study extends the literature by identifying five specific demographic (age, education) and psychological (privacy concerns, online privacy literacy, conspiracy mentality) factors associated with perceived surveillance. Furthermore, this finding is among the first to offer a comprehensive comparison across technological contexts, showing that perceptions of surveillance vary depending on the device or service. These insights highlight the importance of accounting for who the individual is and the technological context in which dataveillance occurs when examining dataveillance effects.

PRACTICAL IMPLICATIONS

The findings from this dissertation have several practical implications for advertisers, ad platforms, and policymakers and regulators. For advertisers, the findings underscore that the extent to which individuals feel surveilled and develop negative attitudes is shaped by the characteristics of the data that are being collected and how they are used. Advertising using personal data, particularly sensitive or extensive personal data, can heighten perceived surveillance and result in more negative attitudes toward the ad, and the brand. Therefore, advertising practitioners should consider not only the personalization effectiveness of data-driven advertisements but also their potential to trigger perceived surveillance and its negative consequences. To find the optimal balance, advertisers should carefully select the type and amount of data used for personalization and avoid using too sensitive or an extensive list of data. For example, our finding shows that personal income, current location, search history, browsing history, and mental health are considered highly sensitive, while languages, hobbies, gender, age, and education are

considered much less sensitive. Moreover, using five types of data can already significantly undermine ad effectiveness comparing to using a single type of data.

Second, perceived surveillance affects not only brands but also ad platforms. Platforms like Google and Meta gather data from individuals, compose algorithmic profiles of individuals, and deliver data-driven advertising through their channels. These platforms rely on dataveillance to make profit and therefore also face critical challenges. We found that people who feel surveilled from viewing their accurate algorithmic profiles also feel more inclined to adjust their privacy settings, limiting future possibilities of data collection. Moreover, when individuals are exposed to data-driven ads using sensitive data or multiple types of data, they develop negative attitudes to the ad platform as well. In the long run, excessive dataveillance might drive users away from these platforms and opt for more privacy-conscious alternatives (Saravanos et al., 2022). To avoid such risks, platforms should be more conscious and selective with what they collect and how they use the data, adopt more responsible data practices, and provide users with more meaningful, visible, and easy-to-use control options.

Third, findings of this dissertation have direct relevance for policymakers and regulators. Although the current regulation in the European Union prohibits the use of special categories of data for ad targeting (General Data Protection Regulation, 2016), using certain types of data outside these categories that are relatively sensitive (e.g., income level, current location, search history, and browsing history) can still cause the feeling of surveillance among individuals. Therefore, the current list of special categories data might need to be expanded. We also found that not only sensitivity but amount of data influences perceived surveillance, yet the current Digital Services Act only requires the disclosure of "main parameters" of personal data used for data-driven advertising (Digital Services Act, 2022, Art. 26). It is therefore important for the current regulations to be updated such that companies must disclose the full range of data used for advertising for consumers to make fully informed decisions. Furthermore, despite the fact that perceived surveillance can contribute to higher intentions to protect privacy, it could also lead to increased privacy cynicism. Although privacy cynicism did not consistently emerge as an immediate response to perceived surveillance in this dissertation, there is a potential that long-term exposure to dataveillance could contribute to citizens' disengagement from privacy protection and erode their agency. It is therefore imperative for policymakers and regulators to limit the scope of dataveillance (e.g., by further limiting the type and amount of data allowed to be used for advertising) and enforce companies to provide accessible and effective features and tools of privacy protection.

LIMITATIONS

This dissertation is not without limitations. First, all the empirical evidence from this dissertation came from cross-sectional studies. While this allowed us to investigate the triggers, consequences, and factors surrounding perceived surveillance in multiple settings and establish many relationships that have never been observed, we are unable to map the dynamic relationships over time with the current data. For instance, the relationship between perceived surveillance and privacy cynicism might accumulate or evolve with repeated exposures to dataveillance, which can only be captured through a longitudinal study. Future research should expose individuals to multiple surveillance episodes over an extended period and incorporate repeated measures to examine the long-term, dynamic dataveillance effects.

Second, this dissertation mainly relied on self-reported measures, as many factors we investigated could only be observed through self-reports, such as perceived surveillance itself, coping strategies, ad evaluations, and psychological factors related to perceived surveillance. However, we also only measured intentions of privacy protection behavior instead of actual behavior. While intentions are a strong predictor of behavior, they do not always translate into action (Sheeran & Webb, 2016). Furthermore, using only self-reported data limited the scope of research questions we could ask. For example, we were not able to examine whether perceived surveillance is related to people's actual uses of digital technologies. Future studies could overcome this by incorporating collections of digital trace data, through tracking or data donation (Ohme et al., 2024).

Third, the studies in this dissertation were conducted with samples from the Netherlands and the United Kingdom, mostly recruited via online panels. This means that some of the current findings might be country and population-specific, or more applicable to individuals with medium-to-high digital literacy. For example, the beliefs about dataveillance might be different in other countries. While corporate surveillance is perceived as most prominent by Dutch individuals, individuals in countries with more prevalent state surveillance might hold different views (Kalmus et al., 2022). Additionally, individuals' privacy regulations, privacy concerns, and knowledge might also differ across countries (Z. Liu & Wang, 2018; Zhang, Voorveld, et al., 2024). Therefore, the findings may not be generalizable to populations with different regulatory and cultural backgrounds. Cross-country research is needed to understand how dataveillance perceptions and responses vary globally (e.g., Segijn et al., 2025). Moreover, since the findings are drawn from samples that were generally digitally literate, their beliefs and responses (particularly coping responses) might differ from those with relatively low digital literacy. Future research should include samples with more diverse range of digital literacy for more generalizable results.

WHAT'S NEXT

This dissertation offers several avenues for future research. First, building on the finding that digital data-driven advertising is a primary driver of perceived surveillance, future studies should continue to investigate dataveillance effects within this context. For advertising scholars, it is crucial to acknowledge and further explore the role of perceived surveillance and its negative impact on advertising effectiveness.

Second, research could also examine how other types of surveillance episodes and their specific features trigger perceived surveillance, for example, through interactions with chatbots, virtual reality, or recommender systems. Chatbots might be used to discuss mental health topics, making the data collected more sensitive and intimate (de Bruijn et al., 2025). Virtual reality is a highly immersive and interactive environment that offers new affordances for data collection and might in turn be used to deliver new types of surveillance episodes (van Berlo et al., 2025). Recommender systems are another context where recommendations can be too accurate and make people feel creepy (Torkamaan et al., 2019).

Third, while this dissertation conceptualizes cognitive coping strategies, privacy protection intention and ad responses as direct responses to perceived surveillance, the relationships between the coping strategies identified in this dissertation and actual privacy protection behavior as well as ad responses might be worth investigating. It was theorized that cognitive coping such as privacy cynicism might be a way for individuals to manage the discomfort of perceived surveillance without taking behavioral action (Hoffmann et al., 2016). Future research should investigate if these coping mechanisms reduce the likelihood of engaging in protective behaviors. In addition, as using resistance strategies to cope with persuasion attempts could result in lower brand attitude and purchase intention (van Reijmersdal et al., 2016), using coping strategies for perceived surveillance might also mediate the relationship between perceived surveillance and ad responses.

Fourth, researchers could explore how to leverage perceived surveillance to encourage privacy-protective actions without simultaneously inducing privacy cynicism. As we see that perceived surveillance is positively related to privacy protection intention, we might be able to leverage perceived surveillance to develop more effective intervention strategies to increase privacy protection behaviors. Boerman et al. (2024) developed successful training strategies that teach users how to take specific actions, which increased privacy protection behavior. However, the strategy aimed at increasing the threat appraisal (i.e., how severe individuals perceive something as a threat, and how susceptible they believe they are to the threat) was not effective. Eliciting perceived surveillance might be a way of raising threat appraisal as individuals who feel surveilled

are highly aware of the ongoing dataveillance practice, contributing to a more effective intervention design. However, the intervention should be carefully designed in a way that it does not also raise privacy cynicism, for example, by providing users with clear, actionable steps and training to enhance their sense of self-efficacy and response efficacy.

IMPLICATIONS FOR EVERYBODY

Are our phones constantly listening to us? Perhaps it does not really matter whether they are listening or not. What matters more is the feeling it triggers—the feeling of being surveilled. This dissertation studies this perception that many individuals have experienced: perceived surveillance, which also offers several implications for individual users.

First, an examination of the perceived benefits and costs of dataveillance reveals that benefits seem to be more personal, realistic, and immediate. While it is certainly fair to enjoy the benefits brought by dataveillance, it is also important to not underestimate its costs even though they seem distant and less personal. It is important to be more conscious of the privacy decisions that are made and consider both benefits and costs.

It is also helpful to be aware of the coping strategies one might adopt when feeling surveilled, such as thinking in the pattern of "there is no point in protecting my personal data." While it may feel overwhelming to realize how much data companies collect from individuals, there is always a point in protecting one's personal data, as it is the only effective way to limit the extent of dataveillance.

With this, this dissertation hopes to encourage every user to take up their agency in the digital environment, by making informed privacy decisions, actively managing their data, and challenging the normalization of dataveillance in their everyday lives.