Feeling watched

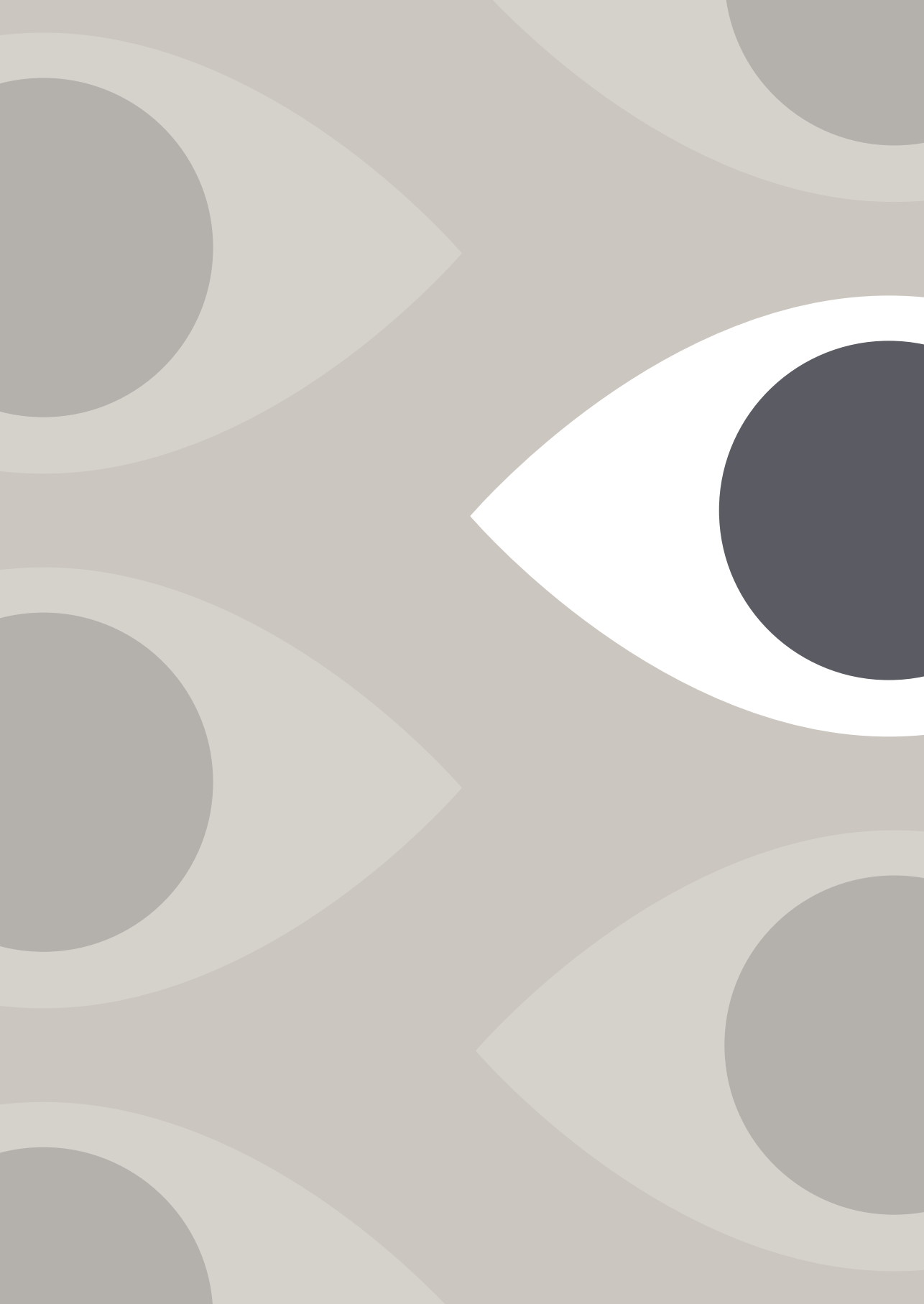
Understanding triggers of and responses to perceived surveillance in digital technologies

Zhang, D.

Publication date
2026

CHAPTER 1

INTRODUCTION



It was a sunny afternoon. My partner and I had just left an independent cinema, both feeling inspired by the arthouse film we had just watched. As we wandered through the city streets, I turned to him. "I really liked that film," I said. "Maybe we should watch more arthouse movies!" He nodded, already pulling out his phone. "Yeah," he replied, "I've heard of an app called MUBI. It's supposed to be specialized in arthouse films. Maybe we could get a subscription."

Hours later, I was at home, relaxing on the couch and casually scrolling through Instagram. My thumb paused mid-scroll, as an ad stared back at me from the screen: "MUBI: subscribe today for €1 for the first three months!"

"Seri—seriously?!" I sat up and shoved the phone in front of my partner's face. "We literally just talked about this!" Before he could react, from the bookshelf behind us, our Apple HomePod lit up. In its calm, polite voice, Siri offered an unsolicited response: "Sorry, I don't know how to respond to that." We looked at each other, eyebrows raised.

But the sense of unease lingered. I took back my phone, opened Google, and began typing: "is my ph..." Before I could finish, the first autocomplete suggestion appeared: "is my phone listening to me." How could it know that I wanted to type that?!

This sequence of events, while personal, is far from unique. Many individuals have experienced similar situations where they got ads that were seemingly related to their recent offline conversations, wondered if their smartphones or smart speakers were always listening, or received personalized recommendations that were way too accurate (Lau et al., 2018; Segijn, Strycharz, et al., 2024; Torkamaan et al., 2019). In situations like these, people feel that they are being watched, listened to, or having their personal data recorded, a perception known as perceived surveillance (Segijn et al., 2022).

Perceived surveillance, also referred to as a sense of dataveillance (Büchi et al., 2022), is conceptualized as a reaction when individuals observe or assume that their personal data are being collected (Strycharz & Segijn, 2022). This feeling prevails widely, as people are increasingly aware that their data are being collected and used. A recent survey in the Netherlands shows that the majority (77%) of Dutch adults are familiar with the collection, use, and sharing of information about their media behavior (Boerman & Segijn, 2022). This perception of surveillance is also reflected through popular media, such as the Netflix documentary The Social Dilemma, which dramatizes the constant dataveillance by social media platforms and critiques its negative impacts (Orlowski, 2020).

Within academia, a growing body of research has begun to conceptualize perceived surveillance, mostly within the context of digital data-driven advertising (e.g., Farman et al., 2020; Frick et al., 2021; Segijn et al., 2022; Segijn & van Ooijen, 2020). However, despite this growing recognition, critical gaps exist in our understanding of this perception. Much

remains unknown regarding its triggers—What exactly causes this feeling? Its consequences—What does it lead to? The broader range of thoughts and feelings people hold when they experience it—What are people's beliefs? And the internal and external factors related to it—Which individual differences or specific contexts are associated with a heightened level of perceived surveillance? This dissertation aims to address these questions, providing a comprehensive understanding of perceived surveillance and its role in explaining the relationship between individuals' dataveillance experiences and responses to dataveillance and data-driven advertising in the dataveillance society.

BACKGROUND AND GENERAL OBJECTIVES: UNDERSTANDING PERCEIVED SURVEILLANCE IN THE DATAVEILLANCE SOCIETY

To understand perceived surveillance, it is crucial to first understand the broader digital landscape from which this perception emerges—the dataveillance society we live in. Dataveillance refers to the automated, continuous, and unspecific collection, storage, and processing of digital traces to regulate or govern the behavior of individuals or groups (Büchi et al., 2022; Clarke, 1988; Strycharz & Segijn, 2022). In today's digital world, every single click, every search query, every second spent on a webpage, every GPS ping, and every time our device is close to another device, tells a little bit about ourselves—what type of content we find interesting, what products we want to purchase, where we live and where we go to work, with whom we just spent some time together. This wealth of information is systematically collected by companies, governments, and other parties for various purposes (Marx, 2015).

Dataveillance is increasingly used for the commodification of personal data to predict and influence human behavior for profit. This has become a new form of economic logic known as surveillance capitalism (Zuboff, 2019). (Big) Technology platforms like Google, Meta, and Amazon collect massive amounts of behavioral data from individuals. These data serve as "raw materials" for building detailed algorithmic profiles (i.e., compilations of data referring to individuals; Büchi et al., 2023) of users and predicting their future actions—what they are likely to click, buy, watch, or support. The predictions are then turned into profits through data-driven advertising and other business models. To maximize profits, companies continuously seek to expand the scope of their data collection, from web browsing and social media to smart wearables and smart home devices, making dataveillance increasingly pervasive (Curran, 2023). This means that individuals are exposed to more and more personalized advertisements and recommendations, and are engaging with increasingly personalized digital services.

Through these experiences, individuals become aware of the collection and use of their personal data and develop the feeling of being surveilled (Strycharz & Segijn, 2022).

As individuals navigate this digital environment, they form their own understandings of how dataveillance works and develop their own judgements of whether this is a good or bad thing. Merely a decade ago, shocked by the Snowden revelations, the public was heavily concerned about state surveillance (Bakir et al., 2015). However, nowadays, people seem to be much more creeped out by a multitude of companies' dataveillance practices (KPMG, 2023). This might point to an increasing prominence of corporate surveillance in shaping people's understandings of dataveillance. Moreover, while scholars criticize the power asymmetry between data collectors and individuals, the undermining of personal autonomy, and the threat to trust and credibility (Andrejevic, 2014; Susser et al., 2019; van Dijck, 2014), we do not know if individuals perceive the same harms. At the same time, individuals may perceive multiple benefits (Strycharz, van Noort, et al., 2019). It is time to update our knowledge regarding what people believe about dataveillance.

Understanding people's beliefs about dataveillance is the first step in understanding perceived surveillance. The next step is to identify what exactly triggers perceived surveillance. People experience perceived surveillance when they observe instances of data collection (Strycharz & Segijn, 2022). In this process, factors related to the data, such as what data are collected, how much data are collected, and how the data are used, could make some instances perceived to be more "surveilling" than others. Not every type of data is considered equally acceptable to be collected and used (Kozyreva et al., 2021). For example, gender and age are generally considered acceptable to be used for personalization, while sensitive information like personal tragedies or household income are strongly opposed to (Kozyreva et al., 2021). Using a combination of personal information rather than a single type can also put people at unease (De Keyzer, van Noort, et al., 2022). In light of that, we look at the specific characteristics of the instances in which people feel surveilled.

Once perceived surveillance is triggered, it can subsequently influence how individuals respond to data-driven advertising. Existing research has extensively examined how perceived surveillance influences ad effectiveness and brand evaluations—when people feel surveilled, they tend to avoid the ad, show more resistance, and have more negative attitudes toward the ad and brand (Farman et al., 2020; Segijn, Kim, & van Ooijen, 2024; Segijn et al., 2023; Sifaoui & Segijn, 2025). However, it can be easily overlooked that most data-driven ads are delivered on a third-party platform, be it a social media platform or a website. Who is there to "blame" when both the brand and platform could be involved in collecting individuals' personal data for advertising? This dissertation considers multiple parties that could be held responsible for dataveillance, not only adding more empirical

evidence on the impacts of perceived surveillance on ad and brand evaluations but also providing novel insights into its effect on platform evaluation.

Meanwhile, scholars have noted a rising sense of futility shared among individuals living in this dataveillance society: They feel that their efforts to protect their privacy in this dataveillance-prevailing environment are unlikely to succeed—an attitude variably termed as privacy cynicism, digital resignation, etc. (Draper et al., 2024). Or they shrug off the privacy risks with the rhetoric of "I've got nothing to hide" (Marwick & Hargittai, 2019; Solove, 2007). These attitudes can be conceptualized as coping strategies that allow individuals to continue engaging in online activities (Hoffmann et al., 2016). But what exactly are these coping strategies addressing? It might be that people adopt these coping strategies in response to perceived surveillance (Strycharz et al., 2022). Besides advertising evaluations, perceived surveillance might also be a driver for responses toward dataveillance itself.

Lastly, there remains the question of whether perceived surveillance is experienced uniformly by everyone in every context. It is plausible that the intensity and likelihood of feeling surveilled may differ significantly from person to person and across various contexts. For example, individuals' privacy concerns are positively related to their awareness of the collection, use, and sharing of media behavior (Boerman & Segijn, 2022). This in turn may indicate a relationship between privacy concerns and perceived surveillance. Additionally, with emerging new technologies offering new affordances, such as microphones built into every smartphone and smart speaker that technically allow for "listening in," individuals might feel particularly surveilled when using certain devices or services.

These observations and potential relationships highlight multiple unexplored areas to be investigated surrounding perceived surveillance, from individuals' beliefs, its triggers, its consequences, to the related individual and contextual factors. Despite the growing relevance of understanding perceived surveillance in this dataveillance society, we lack empirical evidence on many of these fronts, which is what this dissertation aims to provide. To better understand and examine these complex dynamics, this dissertation builds on an existing theoretical framework that explains the mechanisms through which dataveillance influences individuals' perceptions and responses.

THEORETICAL FRAMEWORK: WHAT'S THE DEAL

This dissertation is theoretically grounded in the dataveillance effects in advertising landscape (DEAL) framework developed by Strycharz and Segijn (2022). The DEAL framework explains the process through which individuals' perceptions of dataveillance

can be activated by exposure to dataveillance practices and subsequently impact their responses to digital data-driven advertising and dataveillance. While the framework is built with a focus on the context of digital data-driven advertising, its concepts and the proposed relationships can be applied to the broader context of dataveillance. This framework is particularly central to the current dissertation as it comprehensively outlines the crucial concepts necessary for understanding individuals' perceptions of surveillance and postulates their relationships: surveillance beliefs, surveillance episodes, perceived surveillance, surveillance responses, and ad responses. These concepts will be defined and explained in the research gap sections where they become relevant. Table 1 presents the key concepts adopted from the framework and their definitions.

Table 1

Key concepts of DEAL framework and definitions

Concept	Definition
Surveillance beliefs	The ideas an individual holds regarding the extent and aim of surveillance
Surveillance episode	Directly observable instance of data collection
Perceived surveillance	The feeling of being watched, listened to, or having personal data recorded
Surveillance response	Responsive practices that relate to being surveilled
Ad response	Responses toward the advertisement and its sources

DISSERTATION AIMS

In short, the aims of this dissertation are:

1. to map individuals' beliefs about dataveillance
2. to examine the specific triggers of perceived surveillance
3. to investigate the consequences of perceived surveillance for individuals' coping strategies and responses to data-driven advertising
4. to explore individual differences and contextual factors related to perceived surveillance

These aims address four research gaps, which are elaborated in detail in the following sections.

Research gap 1: Beliefs about dataveillance

According to the DEAL framework, having surveillance beliefs is a prerequisite for perceived surveillance to be triggered (Strycharz & Segijn, 2022). Surveillance beliefs are ideas a person holds regarding the extent and aim of data collection. They are developed over time in two ways. One way is through external information, like transparency disclosures of dataveillance practices by companies, literacy programs, and the news. The other way is through firsthand or secondhand experiences where individuals believe that dataveillance was taking place. Surveillance beliefs can be as general as being aware that one's data are being collected, processed, and shared for advertising purposes (Boerman & Segijn, 2022), or as specific as believing that one's phone is listening to their offline conversations (Segijn et al., 2025; Segijn, Strycharz, et al., 2024). In this dissertation, we explore two types of surveillance beliefs: (1) conceptualizations of dataveillance, which are about what individuals think dataveillance is and how it works, and (2) evaluations about dataveillance, which are positive and negative thoughts and feelings about dataveillance. Knowing what people believe about dataveillance and how they evaluate these practices can inform us about which situations people are more likely to feel surveilled and how they might respond to it.

Dataveillance encompasses a wide range of phenomena, conducted by diverse parties such as state actors, corporate organizations, and even other individuals or groups, for a multitude of purposes (Marx, 2015). Existing studies have focused on beliefs (in the shapes of both conceptualizations and evaluations) related to specific dataveillance practices, such as personalized advertising, virtual assistants, or algorithmic communication (Bucher, 2017; Ur et al., 2012; Vimalkumar et al., 2021). However, in real life, individuals engage with multiple digital technologies simultaneously, potentially experiencing various forms of dataveillance concurrently. The current literature thus lacks a holistic view of beliefs about dataveillance. Without this holistic view, it is impossible to compare the prominence of each type of dataveillance and identify evaluations of dataveillance that are shared across contexts for a more comprehensive understanding.

We explore the conceptualizations of dataveillance through the lens of folk theories, which are "intuitive, informal theories that individuals develop to explain the outcomes, effects, or consequences of technological systems" (DeVito et al., 2017, p. 3165). They are based on personal experiences and beliefs but function in place of knowledge (DeVito et al., 2017; Gelman & Legare, 2011). For each folk theory, we inquire about three dimensions: perceived source (who is surveilling), purpose (why are they surveilling), and mechanisms (how do they surveil). Investigating folk theories of dataveillance contributes to our theoretical understanding of the phenomenon as it enables us to compare the prominence of corporate, state, and other forms of surveillance in shaping individuals'

beliefs about dataveillance, thereby adding new knowledge to the current surveillance literature. Additionally, it helps us contextualize the investigations of the subsequent research gaps. Moreover, regardless of the factualness or concreteness of these theories, they can significantly influence people's evaluations about dataveillance and consequently people's responses.

Furthermore, we map individuals' positive and negative evaluations about dataveillance across contexts. These evaluations represent the perceived benefits and costs of disclosing personal information based on the notion of privacy calculus (Dinev & Hart, 2006; Laufer & Wolfe, 1977). Despite that privacy calculus has been conceptualized as a rational process (Dinev & Hart, 2006), we argue that affective evaluations (i.e., feelings) should also be considered when weighing the benefits and costs. By incorporating the affective dimension, we extend the original privacy calculus model to thus capture a more comprehensive set of privacy perceptions. Moreover, an overview of the positive and negative evaluations can inform us how individuals experience dataveillance and may help explain why individuals engage with dataveillance-enabling digital technologies.

Understanding individuals' beliefs about dataveillance is relevant for the development of policy and media literacy programs and for industry and institutional bodies. For example, the factualness and concreteness of the folk theories could inform where media literacy programs should direct their efforts. The evaluative beliefs can inform policymakers about the individual perspectives of the harm of dataveillance. Industry and institutional bodies might also be interested in knowing if they are (or not) the main source of dataveillance perceived by individuals.

This research gap is addressed by chapter 2 and chapter 3 of the dissertation. In chapter 2, we cover the folk theories, thoughts, and feelings about dataveillance in digital media technologies. Chapter 3 complements the qualitative findings of chapter 2 by quantitatively mapping out the perceived sources and purposes of dataveillance, making the findings generalizable to a population.

Research gap 2: Triggers of perceived surveillance

After mapping the general beliefs about dataveillance across contexts, the next gap to be addressed is the lack of understanding on specific triggers of perceived surveillance. The DEAL framework theorizes that exposure to surveillance episodes, which are directly observable instances of data collection, can elicit perceived surveillance among individuals (Strycharz & Segijn, 2022). One example of surveillance episodes could be viewing one's algorithmic profile, which contains inferences about one's interests and sociodemographic categories made by a company. Another example is seeing digital data-driven ads that used one's personal data to target the advertisement.

Previous research that investigated the triggers of perceived surveillance focused on surveillance beliefs, as increased knowledge or awareness of dataveillance could help individuals recognize the surveillance episodes (Segijn, Kim, & van Ooijen, 2024). However, the characteristics of the surveillance episode itself have been largely overlooked. While the DEAL framework posits that exposure to surveillance episodes leads to perceived surveillance, it does not specify how different surveillance episodes might lead to varying levels of perceived surveillance (Strycharz & Segijn, 2022). In a discussion about chilling effects, Büchi et al. (2022) argue that the specifics of the revelation of a dataveillance practice can determine the magnitude of the change in individuals' digital communication behavior. Similarly, the specific characteristics of a surveillance episode may determine the strength of its impact on perceived surveillance. Surveillance episodes can be highly personal and vary significantly, as different types and amounts of data could be collected and used. Furthermore, these data can be used in different manners in the surveillance episodes, such as making accurate or less accurate inferences about an individual. These factors might trigger perceived surveillance to different degrees. To date, only a few studies investigated how the characteristics of the surveillance episodes influence the level of perceived surveillance, focusing on either ad content or the ad transparency information (Sifaoui & Segijn, 2025; Wang et al., 2025). However, the roles of data-related characteristics, including the type of data, amount of data, and the accuracy of inferences based on these data remain unexplored. Investigating these unexplored triggers of perceived surveillance can extend the DEAL framework and provide a more nuanced understanding of what exactly causes perceived surveillance.

Investigating how specific characteristics of surveillance episodes can trigger perceived surveillance offers insights for companies and policymakers. For companies, it is important to know whether their personalization features or transparency features might induce unintended effects (i.e., perceived surveillance). From a regulator's perspective, knowing which characteristics of a dataveillance practice might particularly lead to high perceived surveillance can aid the refinement of the current regulations on data use and disclosure practices.

This dissertation addresses this research gap by examining the roles of four characteristics from two types of surveillance episodes. In chapter 4, we investigate the roles of perceived and objective accuracy of algorithmic profiling on perceived surveillance. Algorithmic profiles could contain accurate or inaccurate inferences regarding their interests and sociodemographic characteristics. Seeing inferences that are highly accurate could be associated with heightened perceived surveillance. In chapter 5, we move on to the context of digital data-driven advertising, where we examine the effects of two key factors that vary across data-driven advertisements: the sensitivity

and the amount of data used in digital data-driven advertising. We argue that higher sensitivity and larger amounts of data can lead to stronger perceived surveillance.

Research gap 3: Consequences of perceived surveillance

If individuals feel that they are being surveilled, there might be important consequences both for themselves and for the companies involved in dataveillance. The DEAL framework outlines two types of consequences of perceived surveillance: surveillance responses and ad responses (Strycharz & Segijn, 2022). Surveillance responses are responses toward the dataveillance practice itself (e.g., privacy protection). Ad responses are responses toward the advertisement in the surveillance episode (e.g., ad attitude). While the DEAL framework identifies these as two general directions for future research, empirical evidence has been relatively sparse, especially regarding surveillance responses. This dissertation aims to offer novel empirical evidence on both fronts.

Regarding surveillance responses, the few existing works mainly examined the effect of perceived surveillance on behavioral responses like chilling effects (the self-inhibition of legitimate media behaviors) and information disclosure behavior (Kappeler et al., 2023; J. Kim et al., 2025; Strycharz & Segijn, 2024), whereas research on privacy protection behavior as a potential response is scarce. Studies have shown that perceived threat can increase privacy protection behavior, and perceived surveillance could be an indication of a high perceived threat (Boerman et al., 2024; Boerman, Kruikemeier, & Zuiderveen Borgesius, 2021). Therefore, this dissertation looks into whether perceived surveillance is related to a higher intention to engage in privacy protection behavior.

Moreover, while it is certainly worthwhile investigating behavioral responses, cognitive and affective responses cannot be overlooked as they might explain individuals' unwillingness or inability to engage in privacy protection behavior (Hoffmann et al., 2016). It has been argued that ongoing dataveillance has contributed to individuals feeling overwhelmed, disempowered, and resigned from protecting their privacy, an attitude often referred to as privacy cynicism, which serves as a cognitive coping mechanism allowing people to continue their digital engagement without ramping up privacy protection efforts (Hoffmann et al., 2016). Such coping strategies could be the result of individuals feeling surveilled. Hence, the current dissertation explores whether perceived surveillance could lead to cognitive responses such as privacy cynicism.

In terms of ad responses, previous studies mainly examined the effect of perceived surveillance on people's evaluations of the ad and brand (Segijn et al., 2023; Segijn, Kim, Lee, et al., 2024; Segijn, Kim, & van Ooijen, 2024; Sifaoui & Segijn, 2025), yet it is unexplored whether perceived surveillance also influences the evaluation of the platform on which the ad is shown (e.g., a social media platform). In practice, the platforms are usually the

ones collecting and controlling the user data, whereby brands are allowed to utilize it for data-driven advertising (Christl, 2017). However, to individual users, it might be ambiguous who is the one surveilling them. It is then important to know who is "blamed" for the dataveillance practice and whether evaluation of the platform is also affected by perceived surveillance.

A deeper understanding of these consequences can have profound practical and societal implications. For ad practitioners (both brands and ad platforms), it is critical to understand the impact of dataveillance on ad responses, as it helps them anticipate the unintended effects of digital data-driven advertising. This understanding is essential for developing more effective, less intrusive, and ultimately more sustainable digital advertising strategies that benefit both the consumers and brands. For regulators, understanding whether and how individuals respond to perceived surveillance through cognitive coping or privacy protection behavior can inform new policy developments that protect individual privacy and empower users in the digital environment. They may also serve as evaluation metrics for the effectiveness of current regulatory measures.

This dissertation provides empirical evidence to both surveillance and ad responses through its Chapter 4 and 5. In Chapter 4, we investigate how perceived surveillance is related to individuals' intention of privacy protection as well as four coping strategies that we identified in Chapter 2 (privacy cynicism, self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation). In Chapter 5, we examine how perceived surveillance influences privacy cynicism as well as attitudes toward the ad, the brand, and the platform displaying the data-driven advertisement.[1]

Research gap 4: Individual differences and contextual factors related to perceived surveillance

Lastly, there is a need for more research on individual-related and contextual factors related to perceived surveillance. The DEAL framework proposes that individual differences and contextual factors might influence how individuals respond to dataveillance (Strycharz & Segijn, 2022). The effect of dataveillance, like any other media effect, depends on the dispositions of an individual (Valkenburg & Peter, 2013). Individual differences might be related to how individuals feel about surveillance and how they respond to it. One study revealed that younger generations tend to experience lower levels of perceived surveillance compared to older generations (Segijn & van Ooijen, 2020). Yet

[1] Within Chapter 5, the first dependent variable is named privacy resignation, as resignation is one of the dimensions within privacy cynicism that is of most interest to the study (Lutz et al., 2020). For conceptual consistency, it is referred to as privacy cynicism in the current chapter and in Chapter 6.

new insights are needed to examine other sociodemographic characteristics and privacy-related perceptions.

The context in which dataveillance takes place might also be related to how much individuals feel surveilled. Knowledge on the contextual factors that influence perceptions of dataveillance is currently lacking, with only one study showing the roles of different data collection techniques for personalization (Segijn & van Ooijen, 2020). As mentioned before, consumers nowadays engage in digital activities through a variety of digital technologies. Thus, dataveillance practices can take place in broad contexts—seeing personalized ads on social media, a smart watch reminding the user to stand up since they have been inactive, or Google maps asking how crowded the metro they just took was. These may all function as surveillance episodes as people might become aware of the collection and processing of personal data, and experience perceived surveillance. However, do people feel equally surveilled in all these contexts? Which contexts make people more surveilled than others? This is important to know because a difference in the level of perceived surveillance across different contexts might indicate systemic differences that should be taken into account when studying dataveillance effects.

Understanding how individual differences and contextual factors shape perceived surveillance also has important practical implications. For policymakers, these insights can help identify groups that might be more vulnerable to dataveillance. In addition, they help identify which digital technologies are particularly surveilling, and in which instances. In both cases, these insights help inform theory-driven, evidence-based privacy regulations. For advertising practitioners, knowing which platforms or devices evoke stronger feelings of surveillance can guide more ethical and effective targeting strategies. Designers of consumer empowerment interventions can use this knowledge to develop more tailored programs that target individuals with specific traits and contexts of dataveillance. Technology developers can also apply these findings to create more transparent and user-friendly digital experiences.

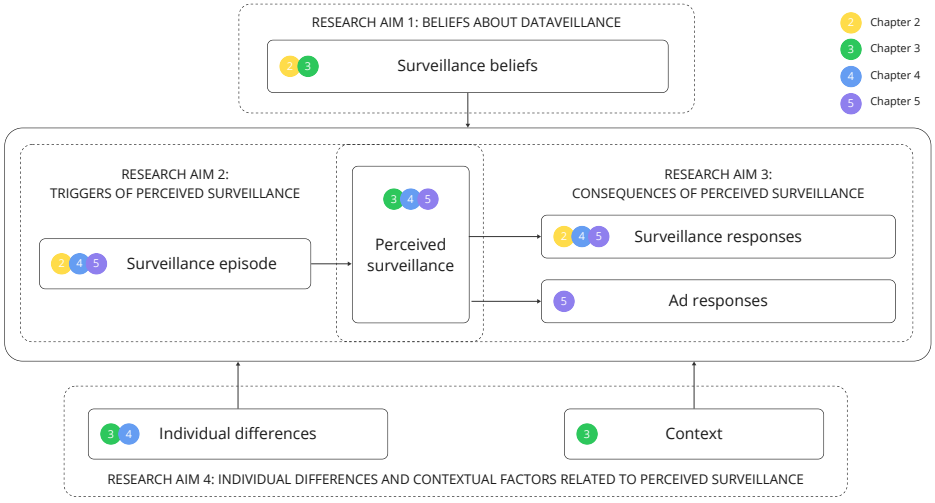
To explore the roles of individual differences, Chapter 3 examines the relationship between perceived surveillance and a number of individual characteristics, including privacy concerns, technology trust, conspiracy mentality, age, gender, and education. Chapter 4 examines how online privacy literacy influences the relationship between perceived surveillance and surveillance responses, identifying the boundary conditions of the effect. To study the role of context, Chapter 3 investigates whether and how the levels of perceived surveillance differ between different digital devices and services that are commonly used by consumers, including smartphone, smart watch/wristband, smart speakers, smart home devices, web browser, social media, navigation app, and virtual assistant.

DISSERTATION OUTLINE

This dissertation consists of six chapters: an introduction chapter (Chapter 1, the current one), four empirical chapters (Chapter 2, 3, 4, and 5), and a discussion and conclusion chapter (Chapter 6). The aims of this dissertation are addressed through the four empirical chapters. Each of the four empirical chapters presents a standalone research study conducted separately and can be read individually as a research article. A summary of each chapter is provided below. Figure 1 is a conceptual model of the dissertation based on the DEAL framework, with the research aims and chapter numbers mapped onto the framework.

Figure 1

Overview of the dissertation structure and research aims



Chapter 2: Folk theories, thoughts, and feelings about dataveillance in media technologies

Chapter 2 presents findings from in-depth interviews with 23 Dutch adults with varying age, gender, technology use, and technology proficiency. It addresses our lack of knowledge on beliefs about dataveillance (Research Gap 1) by mapping out the folk theories, thoughts, and feelings about dataveillance. Folk theories inform us how people make sense of dataveillance. Specifically, each folk theory consists of three dimensions: perceived source, perceived purpose, and perceived mechanism of dataveillance. We then explore what thoughts and feelings people hold about dataveillance, categorized by their

positive and negative valence, reflecting the perceived benefits and costs of being subject to dataveillance.

Chapter 3: Perceived sources and purposes of surveillance; individual differences and contextual factors differentiating perceived surveillance

Chapter 3 presents findings from a cross-sectional online survey with a representative sample of the Dutch adult population (*N* = 1,994). It first complements Chapter 2 to further address the knowledge gap on beliefs about dataveillance (Research Gap 1) by quantitatively describing the perceived sources and purposes of dataveillance, which are two key dimensions of folk theories. Furthermore, to offer insights into individual differences and contextual factors related to perceived surveillance (Research Gap 4), it investigates how multiple individual differences as well as technological contexts relate to the level of perceived surveillance among individuals. Individual differences included privacy concerns, technology trust, conspiracy mentality, age, gender, and education. The technological contexts included smartphone, smart home device, smart watch, smart speaker, web browser, social media, navigation app, and virtual assistant.

Chapter 4: Algorithmic profiling and perceived surveillance, and how people cope with it

Chapter 4 is situated in the context of algorithmic profiling, which is the systematic and purposeful process of recording and classification of data related to individuals (Büchi et al., 2020). This process is the necessary building block of digital data-driven advertising. Through a cross-sectional survey (*N* = 685), we confront users with their personal algorithmic profiles to explore the extent to which perceived and objective accuracy of algorithmic profiling is related to perceived surveillance, advancing our understanding of triggers of perceived surveillance (Research Gap 2). It furthermore disentangles the relations between perceived surveillance and the intention to adjust ad settings (a type of privacy protection behavior) as well as four coping mechanisms identified in Chapter 2, including privacy cynicism, self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation, which provides crucial insights into the consequences of perceived surveillance (Research Gap 3). Moreover, this chapter examines the role of online privacy literacy on the relationship between perceived surveillance and coping strategies, further contributing to our understanding of the roles of individual differences (Research Gap 4).

Chapter 5: Digital data-driven advertising and perceived surveillance, and how people respond to it

Informed by findings from Chapter 2 and 3, digital data-driven advertising is identified as the most common surveillance episode triggering people's feeling of surveillance. Chapter 5 zooms into the context of digital data-driven advertising and investigates two key factors in a digital data-driven advertisement that could influence perceived surveillance: the sensitivity and amount of data used for advertising through a 2 (data sensitivity: low vs. high) × 2 (data amount: single vs. multiple types) online experiment (N = 1,256), which offer critical insights into the triggers of perceived surveillance (Research Gap 2). Furthermore, to further contribute toward a comprehensive understanding of the consequences of perceived surveillance (Research Gap 3), it assesses the influence of perceived surveillance on three types of advertising responses (attitude toward the ad, brand, and platform) as well as privacy resignation, a key component of privacy cynicism.

Chapter 6: Discussion and conclusion

Chapter 6 concludes this dissertation with a general discussion and conclusion. First, it presents a summary of the research findings from Chapter 2, 3, 4, and 5. Then, the theoretical, methodological, and practical implications are discussed, and limitations and directions for future research are addressed.