The future of dataveillance in advertising theory and practice

Strycharz, J.; Segijn, C.M.

DOI
10.1080/00913367.2022.2109781

Publication date
2022

Document Version
Final published version

Published in
Journal of Advertising

License
CC BY-NC-ND

Citation for published version (APA):
The Future of Dataveillance in Advertising Theory and Practice

Joanna Strycharz\textsuperscript{a}\textsuperscript{*} and Claire M. Segijn\textsuperscript{b}\textsuperscript{*}

\textsuperscript{a}University of Amsterdam, Amsterdam, the Netherlands; \textsuperscript{b}University of Minnesota, Twin Cities, Minnesota, USA

ABSTRACT

Technological developments have changed the advertising landscape by extending the possibilities to collect, process, and share consumer data to optimize advertising. These developments have made data collection and consequently dataveillance—the automated, continuous, and sometimes unspecific collection, storage, and processing of digital traces—central concepts for advertising scholarship and practice. Studying the impact of consumers’ perceptions of dataveillance is important as perceptions about data collection practices have been shown to diminish the effects of data-driven advertising. This article advances advertising theory by conceptualizing the impact of consumers’ perceptions of dataveillance in digital data-driven advertising and applying long-standing advertising research theories to this new phenomenon to provide an overarching framework for future research. The current work presents the dataveillance effects in advertising landscape (DEAL) framework, with specific research directions for future research. This framework has practical implications as it shows how false or accurate beliefs about dataveillance impact consumer responses to digital data-driven advertising. Advertisers may adapt to ensure that digital data-driven advertising does not result in backlash or raise ethical questions. Finally, the framework has implications for privacy regulations, as consumer understanding of data collection is a core issue in current regulatory approaches to dataveillance.

Over the years, technological developments have played a crucial role in the emergence and evolution of new forms of advertising. Advertising scholars and the industry have been adapting to new technological advances by changing the definition of advertising and adjusting its practice (Dahlen and Rosengren 2016; Richards and Curran 2002). The same can be said about recent advances in machine-learning algorithms and artificial intelligence (AI), which are currently dominating forces in the advertising industry (Li 2019; Rodgers 2021). They have transformed the advertising ecosystem and have led to the rise of so-called digital data-driven advertising strategies, such as computational advertising and personalized advertising (Table 1). One of the characteristics that distinguishes these types of advertising is the centrality of the collection and processing of consumers’ behaviors and personal characteristics. Computational advertising strongly depends on granular-level data collection, mining, and aggregation (Helberger et al. 2020). Hence, recent developments in the advertising practice contribute to dataveillance—or the automated, continuous, and unspecific collection, storage, and processing of digital traces (Büchi, Festic, and Latzer 2022; Degli-Esposti 2014). However, a comprehensive overview of the impact of consumers’ perceptions of dataveillance on advertising effects is largely missing.

Consumers have been shown to feel uneasy that their data are so widely collected and processed for advertising purposes, as such harvesting poses a threat to their privacy (Segijn and Van Ooijen 2022) and autonomy (Solove 2007; Büchi, Festic, and Latzer 2022). The impact of consumers’ perceptions of dataveillance is important to study for advertising practice

CONTACT Joanna Strycharz j.strycharz@uva.nl Amsterdam School of Communication Research, University of Amsterdam, Nieuwe Achtergracht 166, 1018WV Amsterdam, the Netherlands.

*Both authors contributed equally.

Joanna Strycharz (PhD, University of Amsterdam) is an assistant professor, Amsterdam School of Communication Research, University of Amsterdam.

Claire M. Segijn (PhD, University of Amsterdam) is an associate professor, Hubbard School of Journalism and Mass Communication, University of Minnesota.

© 2022 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.
as awareness of data collection practices and privacy threats in general are known to diminish the effects of data-driven advertising by inducing cognitive, affective, and behavioral responses among consumers (e.g., Ham 2017). Hence, the aim of this article is to conceptualize the impact of consumers’ perceptions of dataveillance in digital data-driven advertising and apply long-standing theories in advertising research to this new phenomenon to provide an overarching framework for future research on this topic.

This article contributes to building our understanding of digital data-driven advertising by theorizing the role of consumers’ perceptions of dataveillance in the advertising landscape. Based on existing theories in advertising—most of which were developed before the digital advertising era—we build a framework that could drive future research on digital data-driven advertising. Given the omnipresence of data and its usage for advertising (Huh and Malthouse 2020; Yun, Segijn, et al. 2020), it is expected that dataveillance will be central to the future of advertising practice. Therefore, we propose the dataveillance effects in advertising landscape (DEAL) framework, which is expected to serve as a framework to study consumers’ perceptions of dataveillance in digital data-driven advertising in the years to come. This framework is patterned on the persuasion knowledge model (Friestad and Wright 1994) but is different because (1) the focus of DEAL is on a surveillance episode, (2) DEAL introduces the idea of surveillance beliefs, and (3) DEAL includes surveillance responses as a unique way to respond to digital data-driven advertising which is different from general advertising responses. We start by conceptualizing dataveillance and its role in the digital advertising landscape. Next, we discuss the DEAL framework embedded in theory and research relevant to the advertising scholarship. Finally, building on the DEAL model, we propose an agenda for future research on the role of consumers’ perceptions of dataveillance in advertising.

The DEAL framework also has implications for advertising practitioners and regulators. For advertisers, it shows how false or accurate surveillance beliefs impact consumer responses to digital data-driven advertising and where these beliefs may possibly stem from. This allows advertisers to correct them and to ensure that digital data-driven advertising has the intended positive effects and does not result in a backlash. It also allows advertisers to anticipate possible ethical implications of digital data-driven advertising. In addition, the DEAL framework has important implications for privacy regulations, because consumer understanding of data collection and processing practices is a core issue in current regulatory approaches to dataveillance.

Setting the Scene

Defining Dataveillance

Based on the definitions provided by Degli-Esposti (2014) and Büchi, Festic, and Latzer (2022), we define dataveillance as automated, continuous, and (un)specific collection, storage, and processing of digital traces from people or groups, by means of personal data systems by state and corporate actors, to regulate or govern their behavior. Companies across various sectors have been collecting, using, and sometimes sharing information about prospects and consumers for decades. As a result, these companies have become the main sources of (continuous) data collection in the digital society (Christl 2017). Central to this definition is that the purpose of data collection is to regulate or govern behavior. This includes advertising and other practices of organizations aimed at persuading consumers, and hence makes dataveillance different from simple online monitoring or analytics, which focus on identification of relevant audiences or gaining insights about consumers (Andrejevic 2006). In addition, volume, velocity, variety, and continuousness make it different from the concept of data collection (Table 1).

Before digital developments, four main sources of consumer data existed. First, companies kept their own records on consumers (e.g., through loyalty programs). Second, in the direct marketing sector, lists of consumers with certain characteristics were commonly traded. Third, credit bureaus held detailed credit information on consumers. And fourth, records about individuals such as birth certificates and various licenses were available to companies (Christl 2017). Nowadays, data and analytics companies commonly combine information from all four of these streams, and digital tracking enables the collection of additional information about consumer behavior and characteristics that was not accessible in the past.

For years, tracking of online behavior has been widely used to collect information about people. Technological solutions such as cookies have enabled companies to track website visits and follow the online behavior of individuals (Smit, Van Noort, and Voorveld 2014). More recently, we are also observing the extension of data collection from the digital context to the offline world (Christl 2017; Yun, Segijn, et al. 2020). Devices such as smartphones, wearables, and other smart devices that are equipped with sensors and connected to the Internet are used to make possible today’s tracking and profiling landscape, adding another dimension to the extent of data collection (Christl 2017). This
continuous collection of data about online and offline behaviors of consumers through a magnitude of devices contributes to the creation of dataveillance.

**Dataveillance and Advertising**

Digital data-driven advertising that relies on processing consumer data to create and deliver advertising messages and to measure their effects (Huh and Malthouse 2020; Yun, Segijn, et al. 2020) is one of the factors contributing to the creation of dataveillance (Degli-Esposti 2014). In exchange for free services (e.g., web searches, social networks), organizations develop profiles of consumers who use their services and use or sell such information to other companies, either in the form of data or as market segments tailored for ad placement. Based on the combined data of (among others) past search behavior, past browsing behavior, products viewed online, articles read, and videos watched, ads can be adjusted to individual consumers across a network, with the aim of making them attractive and personally relevant to the individual (Yun, Segijn, et al. 2020). Due to the importance of data in the current advertising landscape, technology companies that create consumer profiles are now seen as a part of the refined advertising industry, while data collection technology is seen as a crucial precondition for data-driven advertising (Helberger et al. 2020).

Regarding the future of digital data-driven advertising, data collection technology is expected to shape it and drive its expansion (Helberger et al. 2020). Developments in automated content recognition techniques will make it possible to deliver personalized ads drawing on both offline and online data, such as TV viewing behaviors that are being tracked through watermarking or IP-matching techniques (Segijn 2019), or website visits that are being tracked by cookies or social media pixels (Van Gogh, Walrave, and Poels 2020). The same applies to indoor data collection—in stores, for example. Bluetooth beacons enable advertisers to monitor and react to consumers’ needs and demands (Kwet 2019). Information from smart cars, smart homes, and smart cities are expected to enable further adjustments of ads based on consumer data. Regarding impact on consumers, past research shows that exposure to personalized advertising in the public space (for example, in-store advertising) elicits both positive and negative consumer reactions (Hess et al. 2020). Hence, these developments provide opportunities for advertisers but also raise important questions about how these

---

**Table 1. Glossary of main concepts.**

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Definitions</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computational advertising</td>
<td>&quot;Broad, data-driven advertising approach relying on or facilitated by enhanced computing capabilities, mathematical models/algorithms, and the technology infrastructure to create and deliver messages and monitor/ surveil an individual's behaviors.&quot;</td>
<td>Huh and Malthouse 2020, p. 1</td>
</tr>
<tr>
<td>Data collection</td>
<td>Monitoring of personal information (behavior, interests, traits, beliefs, and intentions)</td>
<td>Acquisti et al. 2015</td>
</tr>
<tr>
<td>Dataveillance</td>
<td>Automated, continuous, and (unspecific) collection, retention, and analysis of digital traces by people or groups, by means of personal data systems by state and corporate actors, to regulate or govern their behavior</td>
<td>Based on Büchi, Festic, and Latzer 2022, Degli-Esposti 2014</td>
</tr>
<tr>
<td>Digital data-driven advertising</td>
<td>Message of persuasion (regarding products, services, or ideas) that interacts with consumers through digital media and requires consumer data to be collected, processed, or stored</td>
<td>Based on Lee and Esposti 2020</td>
</tr>
<tr>
<td>Perceived surveillance</td>
<td>The feeling of being watched, listened to, or having personal data recorded</td>
<td>Segijn et al. 2022</td>
</tr>
<tr>
<td>Personalization/(micro)targeting/tailoring</td>
<td>&quot;The strategic creation, modification, and adaptation of content and distribution to optimize the fit with personal characteristics, interests, preferences, communication styles, and behavior.&quot;</td>
<td>Bol et al. 2018, p. 373</td>
</tr>
<tr>
<td>Surveillance beliefs</td>
<td>&quot;The ideas an individual holds regarding the extent and aim of surveillance&quot;</td>
<td>Based on the concept of beliefs in Yzer 2012</td>
</tr>
<tr>
<td>Surveillance culture</td>
<td>&quot;This term describes how people are not only under surveillance by government or corporate interests—even in our most mundane day-to-day tasks—but also engage and participate in surveillance of other people, like observing others on social media.&quot;</td>
<td>Penney 2021, p. 1511</td>
</tr>
<tr>
<td>Surveillance episode</td>
<td>Directly observable instance of data collection (for example, through a digital ad that is perceived as data driven)</td>
<td>Based on the concept of persuasion episode by Friestad and Wright 1994</td>
</tr>
<tr>
<td>Surveillance imaginaries</td>
<td>Collective understanding of the extent and aim of surveillance and expectations about an individual’s own behavior</td>
<td>Duffy and Chan 2019</td>
</tr>
<tr>
<td>Surveillance response</td>
<td>Responsive practices that relate to being surveilled</td>
<td>Lyon 2017</td>
</tr>
</tbody>
</table>
technologies will affect consumer responses to digital data-driven ads.

**Perceived Surveillance: Effects of Dataveillance on Consumers**

From the societal perspective, dataveillance contributes to the creation of so-called surveillance culture, which is driven by “corporate and state modes of surveillance, mediated by increasingly fast and powerful new technologies, tilted toward the incorporation of everyday life through information infrastructures and our increasing dependence on the digital in mundane relationships” (Lyon 2017, p. 826). Such culture goes beyond the surveillance state, a notion commonly discussed in the 20th century and related to governmental surveillance. Corporations now take a central role in dataveillance as well. The consequence of this surveillance culture for individuals is that they, similar to all other actors in the society, may play an active role in it through their perceptions and behaviors (Lyon 2017). In the past, consumers’ active role in surveillance culture has been shown through self-monitoring behaviors on social media platforms. Users of such platforms adjust their behavior to anticipate the monitoring of others: social media platforms, family, employers, and so on (Duffy and Chan 2019).

From an individual’s point of view, data collection and processing by corporations may trigger one’s perception of being surveilled (i.e., perceived surveillance), which can be defined as the feelings of being watched or listened to, or that personal data are recorded (Segijn et al., 2022). An example of this is the so-called surveillance effect; for example, when interacting with smart devices, consumers worry that their devices listen to them, which results in relevant ads being displayed online based on their recent conversation topics (Frick et al. 2021). Hence, automated and continuous data collection by corporations may lead to the perception among consumers that they are being watched regardless of whether this is true. Table 2 provides an overview of studies that examined perceived surveillance in relation to digital data-driven advertising.

Perceived surveillance may impact individual behavior. More specifically, when their data are being collected, consumers may play an active role in surveillance culture by trying to regulate what others can collect about them and what can be done with this knowledge (Lyon 2017). More specifically, they construct surveillance imaginaries, or a collective understanding of the extent and aim of surveillance and expectations about individual own behavior (Duffy and Chan 2019). In addition, this leads to the implementation of surveillance practices, in other words, the disciplinary and reactive tactics developed as a consequence of feeling surveilled (Duffy and Chan 2019). Hence, surveillance practices are conceptualized as responses by the person being surveilled and not as practices executed by the surveillant. To prevent confusion, we label them surveillance responses, which include consumer behavioral responses to perceived surveillance (Table 1). Due to the central role of dataveillance within data-driven advertising and consumers’ perceptions thereof, surveillance responses can potentially be a new type of responses to advertising.

**Introducing the Dataveillance Effects in Advertising Landscape (DEAL) Framework**

To further our understanding of the role of consumers’ perceptions of dataveillance in the digital advertising landscape and to enable future research in this area, we propose the DEAL framework (Figure 1). Central to this framework is the concept of consumers’ perceptions of dataveillance. The DEAL framework explains how perceptions of dataveillance can be activated by ad exposure and subsequently affect surveillance (e.g., privacy protection) and advertising responses (e.g., brand attitudes, sales, resistance). The starting point of the DEAL model is the surveillance belief that, similar to other cognitive beliefs such as persuasion knowledge (Friestad and Wright 1994; Ham and Nelson 2016), consumers develop over time through different sources. We propose that surveillance beliefs can be activated through a surveillance episode, which is a directly observable instance of data collection. For example, exposure to advertising can lead to the perception of surveillance. That means that when surveillance beliefs are absent or not activated, consumers would not make the link between ad exposure and data collection and thus would not perceive surveillance. Hence, surveillance beliefs are a condition of activation of perceived surveillance.

**Formation of Surveillance Beliefs**

In general, beliefs are ideas that a person holds as being true (Yzer 2012). Hence, we define surveillance beliefs as the ideas a person holds regarding the extent and aim of data collection. In contrast to surveillance imaginaries conceptualized in past research, beliefs are individual and they may differ among consumers. Surveillance beliefs can be information driven (i.e., transparency of practice, education/literacy programs,
media) and experience driven (i.e., firsthand or secondhand experience). Building on past research on beliefs, we argue that they could be created through accurate and false information (Lin and Xu 2021), and therefore surveillance beliefs could be a mix of accurate information and misinformation. However, no matter whether consumers’ beliefs are based on accurate or inaccurate information, they may still be activated by ad exposure and affect subsequent perceptions, attitudes, and behaviors (similar to the impact of other false beliefs on perceptions and behavior; Stasson and Fishbein 1990).

### Information-Driven Surveillance Beliefs

Information-driven surveillance beliefs can be created in at least three ways: transparency of (ad) practice,
education/literacy programs, and the media. First, we argue that surveillance beliefs may be created by transparency of the data collection practices, such as disclosing how corporations collect, process, or share personal data (Segijn, Strycharz, et al. 2021). In the context of digital data-driven advertising, this disclosure could be done by providing detailed information about how personal data are collected and for how long they are kept (Song et al. 2016), including disclosure statements of data collection methods (Van Noort, Smit, and Voorveld 2013; Van Ooijen 2022); providing information on personalization parameters, such as “Why am I seeing this ad?” information (Kim, Barasz, and John 2019); providing information on inferences made from personal data, such as “Your Interests” on Facebook (Büchi et al. 2021) or user agreements when installing a new app (McDonald and Cranor 2008). Transparency practices can be voluntary (in which case the type of information provided is decided by the data collector or processor) or obligatory (in which case the regulators set requirements for such practices, as is the case in the European Union) (Degeling et al. 2019). Either way, the actor responsible for data collection, processing, or sharing is the one responsible for the transparency of these practices (Segijn, Strycharz, et al. 2021). Once consumers are exposed to the disclosure, this may contribute to their surveillance beliefs. Possible exceptions are when disclosures or user agreements are avoided by the consumer, when no attention is paid to the disclosure (Van Noort, Smit, and Voorveld 2013), or when the disclosure is misunderstood or difficult to process (Van Ooijen and Vrabec 2019).

Second, similar to the formation of persuasion knowledge or advertising literacy (Hudders et al. 2017), surveillance beliefs could be created through literacy programs. In fact, it has been argued that in the current advertising landscape consumer understanding of data collection practices is crucial. Hence, regulators and consumer advocates need to take an active role in increasing consumer literacy (Helberger et al. 2020). Previous work on data-driven advertising strategies has shown that knowledge about how these tactics work is often limited (e.g., Segijn and Van Ooijen 2022; Smit, Van Noort, and Voorveld 2014; McDonald and Cranor 2010). However, past research has also shown that, even when consumers do not completely understand data collection, processing, and sharing, they are highly aware that their data are being collected, processed, and shared for advertising purposes, and they perceive these practices as a threat to their privacy (Boerman, Kruikemeier, and Zuiderveen Borgesius 2021; Strycharz et al. 2019, 2021). Hence, consumers may form surveillance beliefs without detailed understanding of data collection practices.

Third, consumers can also learn about data collection practices through the news media. As Von Pape,
Experience-Driven Surveillance Beliefs

When consumers are exposed to an ad that builds on their personal information, this exposure could make them aware that their information has been collected and is now processed to target them with a specific product or service. This is an example of beliefs through firsthand experience (Friestad and Wright 1994). For example, Kim and Huh (2017) found that self-reported exposure frequency to online advertising based on past behavior is negatively related to whether consumers would click on a specific ad; the more ads consumers report seeing daily that are based on their browsing behavior, the less likely it is that they will click on such an ad. In addition, consumers also acquire experience-driven beliefs through conversations with other consumers (secondhand experience) (Friestad and Wright 1994), which could also have consequences for advertising effectiveness.

People use folk theories to understand phenomena in everyday life, such as technological systems (DeVito, Gergle, and Birnholtz 2017), algorithms in the media (Ytre-Arne and Moe 2021), or algorithmic profiling (Büchi et al. 2021). Folk theories are not necessarily based on facts but are formed based on people’s personal experiences (Gelman and Legare 2011). More specifically, they are rooted in experience, rather than mapping more abstract explanations of how technology works (Toff and Nielsen 2018). They can be more or less explicit, purely speculative, based on personal experience, and/or based on secondhand sources (Rip 2019). An example of such a folk theory is the earlier mentioned surveillance effect (Frick et al. 2021). It is argued that due to selective attention for salient items (Klayman 1995), advertising for products one has recently talked about stands out to consumers. This reinforces folk theories because, in general, people look for evidence supporting their existing beliefs (Nickerson 1998). Therefore, we argue that it does not matter whether folk theories are accurate for their impact on one’s surveillance beliefs and subsequent change in surveillance and advertising responses.

Surveillance Responses

When consumers’ surveillance beliefs are activated, consumers may experience the feeling of being watched. For example, when seeing a personalized ad on their mobile device consumers sometimes believe that the ad was shown based on the device monitoring their past conversations (Frick et al. 2021). This may create or activate their belief that “their phone is listening.” This surveillance belief (cognitive belief, even though not necessarily accurate) makes consumers feel watched (i.e., perceived surveillance). Hence, when an ad is brought in relation with data collection, it makes consumers think of their cognitive beliefs that may make them feel watched. Subsequently, perceived surveillance could affect surveillance and advertising responses. Surveillance responses are responsive practices that relate to being surveilled (Lyon 2017). They represent a way to respond to a situation of perceived surveillance. Surveillance responses can be cognitive (e.g., calculus), affective (e.g., emotional responses), and behavioral (e.g., privacy protection measures).

Regarding cognitive surveillance responses, privacy research shows the importance of costs and benefits calculus in the situation of data collection and processing. The so-called privacy calculus theory prescribes that when confronted with collection and processing of their data, consumers balance the associated benefits and costs (Lauffer and Wolfe 1977). These benefits and costs then define their behavioral reaction, for example, self-disclosure or taking privacy protection measures (Baruh, Secinti, and Cemalciar 2017). Benefits include, for example, entertainment, relevant information, or monetary rewards, while costs include potential identity theft, reputational damage, or loss of control over data (Dinev and Hart 2006). A qualitative study showed that people could have positive thoughts related to perceived surveillance, such as the idea that it leads to a better user experience, personal benefits, and admiration about what technology can do (Zhang et al. 2021). Regarding advertising, past research has shown that exposure to a personalized ad can indeed trigger considerations of benefits and costs (Bol et al. 2018).

Second, perceived surveillance can also lead to affective reactions among consumers. For example, Segijn and Van Ooijen (2022) found that respondents expressed negative affect or emotions in their
qualitative answers as a response to a personalization scenario. They found personalized ads and tactics creepy, annoying, or unsettling. Furthermore, they expressed that they disliked, distrusted, or hated them, and that such tactics could make them upset or worried. Besides negative affect, some participants also expressed positive affect or emotions. For example, they mentioned that personalized advertising could make them happy or that it excited them.

Finally, perceptions of surveillance could also result in behavioral surveillance responses by the consumer aimed directly at dataveillance (Lyon 2017). They include limiting the information consumers disclose and adopting privacy protection measures (Boerman, Kruikemeier, and Zuiderveen Borgesius 2021). Regarding limiting disclosures, consumers may choose to self-censor the information they share online in case of voluntary online disclosure, or they may change their behavior to control what behavioral information can be collected about them—so-called chilling effects (Büchi, Festic, and Latzer 2022). Chilling effects can be described as individuals refraining from exhibiting certain behaviors to keep their data from being collected (Solove 2007). In the context of advertising, chilling effects can, for example, include not visiting websites that collect consumer data or not using technology that is perceived as surveilling. By adopting protective measures, consumers actively mitigate the collection, processing, and sharing of their personal information, for example, by installing ad blockers, using incognito browsers when searching for flight tickets, declining or deleting cookies, and using a VPN or “do not track” function (Boerman, Kruikemeier, and Zuiderveen Borgesius 2021). Furthermore, when data are directly shared by consumers—for example, when signing up for a service—consumers can purposely provide inaccurate information to mislead the data collector (Yun, Segijn, et al. 2020).

**Advertising Responses**

Perceived surveillance and surveillance responses could also lead to certain ad responses (e.g., attention, brand memory, brand attitudes, sales, resistance). We argue that while not directly related to the advertisement itself, perceived surveillance may impact advertising responses through spillover effects. Spillover refers to the way that information not mentioned in the message affects ad perceptions and beliefs (Ahluwalia, Unnava, and Burnkrant 2001). For example, Tan, Brown, and Pope (2019) concluded that perceptions about the website on which an ad is shown, such as respect toward the website, positively impacted attitudes toward the advertised brand. Regarding digital data-driven advertising, one could expect that data collection necessary for creation of the ad, while unrelated to the focal information, may influence its effectiveness.

In addition, perceived surveillance could directly result in a form of advertising resistance, which is defined as “a motivational state, in which consumers have the goal to reduce attitudinal or behavioral change or to retain one’s current attitude” (Fransen et al. 2015, p. 7). According to reactance theory (Brehm and Brehm 1981), resistance is experienced when individuals perceive that their freedom is limited by persuasive attempts, such as advertising. Consumers can resist advertising by using avoidance (e.g., changing channels, ignoring), contesting (e.g., counterarguing), and empowerment (e.g., attitude bolstering) (Fransen et al. 2015). Indeed, some initial research found that perceived surveillance increases perceived threat (Farman, Comello, and Edwards 2020), counterarguing (Farman, Comello, and Edwards 2020; Segijn, Kim, et al. 2021), and affective reactance (Farman, Comello, and Edwards 2020). Finally, we propose a link between surveillance responses and advertising responses. For example, experiencing certain emotions (e.g., dislike, hate, distrust) could carry over to the evaluation of the ad message. In addition, taking certain actions (e.g., privacy protection measures) could lead to a false sense of control which could lead to more positive advertising responses by letting one’s guard down. In the context of online disclosure, Brandimarte, Acquisti, and Loewenstein (2013) introduced the notion of a control paradox: Control over sharing private information increases the willingness to publish sensitive information. This paradox could also take place in relation to privacy protection and advertising responses.

**Boundary Conditions**

How consumers respond to dataveillance may depend on individual characteristics and contextual factors. We discuss several individual characteristics that have often been examined in digital data-driven advertising or linked to dataveillance. In addition, we discuss sources, purpose, mechanism, data type, and timing as context factors.
**Individual Differences**

As data collection and processing for advertising purposes increases privacy risks (e.g., McDonald and Cranor 2010), privacy concerns have become a central factor that determines how consumers cope with data collection. Privacy concerns can be defined as “the degree to which a consumer is worried about the potential invasion of the right to prevent the disclosure of personal information to others” (Baek and Morimoto 2012, p. 63). In the past, it has been shown that privacy concerns increase ad skepticism, generate avoidance for personalized advertising, and can also cause less positive attitudes toward such advertising (Kim and Huh 2017; Baek and Morimoto 2012).

Privacy cynicism is another factor that has recently been examined as an individual difference that could affect how people cope with data collection and processing (Van Ooijen, Segijn, and Opree 2022). Privacy cynicism “represents a cognitive coping mechanism, allowing users to overcome or ignore privacy concerns and engage in online transactions, without ramping up privacy protection efforts” (Lutz, Hoffmann, and Ranzini 2020, p. 1173). Past research has shown that individuals who are more cynical put less effort into making privacy decisions and thus are less likely to protect their privacy and instead “do nothing” (Choi, Park, and Jung 2018).

In addition, conspiracy mentality might be relevant to study in this context. Conspiracy mentality is the susceptibility of people to explanations based on conspiracy theories (Bruder et al. 2013). Given that people who are more likely to believe in one conspiracy theory are also more likely to believe in other conspiracy theories (Swami, Chamorro-Premuzic, and Furnham 2010), it is likely that people who score high on conspiracy mentality scales are also likely to believe in, for example, the surveillance effect. Initial research on personalized advertising found that conspiracy mentality contributes to awareness of data collection, processing, and sharing (Boerman and Segijn 2022). Regarding advertising responses, one could thus expect that consumers with conspiracy mentality are, for example, more likely to engage in surveillance responses in reaction to perceived surveillance.

While concerns and perceptions about privacy may have a negative impact on consumers’ responses to advertising, having a positive attitude toward receiving digital data-driven ads may mitigate the effect of perceived surveillance. Data-driven advertising has numerous benefits for consumers, such as informativeness, credibility, and entertainment of the ad (Kim and Han 2014). The privacy calculus theory or privacy trade-off explains this result; when the value of an object, person, or activity outweighs the costs of sharing personal data, consumers are more likely to share their data or accept data collection methods (Acquisti, John, and Loewenstein 2013; Dinev and Hart 2006).

**Contextual Factors**

In terms of contextual factors, Zhang et al. (2021) identified source, purpose, and mechanism as important factors in the discussion of dataveillance. First, the source (i.e., who) is about the actor who is behind the data collection. In our context this is the corporation that collects, processes, and shares the personal data of (potential) consumers. The type of corporation (e.g., sector, size, for profit/nonprofit) and how it is perceived by consumers may influence the effects of perceived surveillance. For example, Bleier and Eisenbeiss (2015) showed that highly trusted corporations can collect and process personal data for advertising purposes without eliciting increased reactance or privacy concerns, which is not the case for less-trusted corporations. In addition, to what extent consumers perceive the source as credible could influence advertising effectiveness. According to the source credibility hypothesis, perceptions about a message rely on perceptions about its source (Hovland and Weiss 1951). Relationship strength (e.g., brand loyalty) with the company may also play a mitigating role in the effects of perceived surveillance.

Second, the perceived purpose (i.e., why) of data collection, processing, and sharing is an important context factor that could influence the relationship between perceived surveillance, and surveillance and advertising responses. For example, consumers could believe that corporations collect their data for financial gain, advertising optimization, product development, manipulating them into certain behaviors (Zhang et al. 2021), security (Van Dijck 2014), or service improvement (Zhu et al. 2017). In line with the privacy calculus theory (Dinev and Hart 2006), consumers might respond differently to a situation of perceived surveillance when they see benefits (e.g., service improvement, security) rather than costs (e.g., manipulation).

Third, the perceived mechanism (i.e., how) that is used to collect, process, or share the information could influence the relationship between perceived surveillance, and surveillance and advertising responses. Segijn and Van Ooijen (2020) showed that different data collection methods result in varying levels of perceived surveillance. In their study, they
examined consumers’ perceptions of online profiling, social media analytics, IP matching, geofencing, keywords, and watermarking. Even though all of these methods were considered to increase perceived surveillance, they varied in the degree of perceived surveillance. Moreover, the older the generation, the more surveilled they felt. Regarding how data are collected, transparency of this process could also impact consumer behavior (Segijn, Strycharz, et al. 2021). For example, when organizations collect and process data openly (so-called overt data collection), consumers react to ads more positively than when organizations collect and process data covertly (Aguirre et al. 2015).

In addition, we include the type of data (i.e., what) that is collected, processed, or shared. Advertising can be personalized based on, among other factors, demographic information (e.g., De Keyzer, Dens, and De Pelsmacker 2015), online behaviors (Smit, Van Noort, and Voorveld 2014), or simultaneous media consumption (Segijn 2019). The type of personal data could affect advertising outcomes depending on the information specificity (Boerman, Kruikemeier, and Zuiderveen Borgesius 2017; Bleier and Eisenbeiss 2015).

Finally, we add when to the list of contextual factors. This factor refers to the timing of data collection, processing, or sharing. Data collection could be seasonal, centered around big events (e.g., Super Bowl, Olympics, holidays) or when consumers are in specific locations, such as when they are in a public or private setting (e.g., home). For example, Strycharz and Segijn (2021) investigated to what extent collecting data on offline behavior of individuals in their homes led to more behavioral surveillance responses due to intrusion of private space of consumers. In addition, the impact of perceptions of dataveillance might be different depending on situations in which consumers are more vulnerable, for example, when they are tired and have less cognitive capacity to think critically and make informed decisions (Strycharz and Duivenvoorde 2021). Also, consider these practices during crisis situations, such as during the COVID-19 pandemic.

**Future Research Agenda**

Research regarding the impact of consumers’ perceptions of dataveillance in digital data-driven advertising is still in its infancy. Given the quantities of consumer data available and the opportunities for the advertising industry, it is expected that research focusing on dataveillance will only increase. Based on the DEAL framework described in the previous section, we propose three areas of future research (Table 3).

**Research Direction 1: Surveillance Beliefs**

Surveillance beliefs play an important role in the DEAL framework. Future research is necessary to further examine (1) how surveillance beliefs are developed or activated; (2) what the effects of these beliefs are; and (3) how to combat false beliefs (e.g., misinformation or conspiracy theories on dataveillance).

**Table 3. Future research directions overview.**

<table>
<thead>
<tr>
<th>Research Direction</th>
<th>Research Topic</th>
<th>Related (Advertising) Theories</th>
<th>Potential Contributions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Surveillance beliefs</td>
<td>How beliefs are developed</td>
<td>Persuasion knowledge model (Friestad and Wright 1994) Covert advertising recognition and effects model (Wojdynski and Evans 2020)</td>
<td>Consumer empowerment through transparency Effectiveness of data collection disclosures</td>
</tr>
<tr>
<td>3. Surveillance responses</td>
<td>Studying chilling effects in response to corporate surveillance</td>
<td>Theory of the chilling effects of dataveillance (Büchi, Festic, and Latzer 2022)</td>
<td>Unintended effects of digital data-driven advertising Identification of groups more likely to show surveillance responses</td>
</tr>
</tbody>
</table>

**Table 3.** Future research directions overview.
Development and Activation of Surveillance Beliefs

First, research should focus on how surveillance beliefs are developed or activated through transparency of practice, education/literacy programs, news media, and firsthand or secondhand experience. Similar to other types of beliefs (Yzer 2012), surveillance beliefs can be measured through a two-step process by conducting a belief elicitation study to identify salient beliefs in the target population first, followed by a survey study in which those beliefs can be linked to, for example, surveillance responses. Regarding transparency of practice, research could further investigate how to best inform consumers about data collection, processing, and sharing practices. The transparency-awareness-control framework (Segijn, Strycharz, et al. 2021) could be used as a starting point for such investigations. To what extent transparency is effective in belief formation depends on how consumers are informed about the practices. Studying characteristics of transparency messaging is a possible future research direction that would contribute to theory building on consumer empowerment through transparency. Also, research could further investigate how to effectively ask consumers about collection, processing, and sharing their information through user agreements in a way that will allow consumers to read them and make them easier to comprehend.

Similarly, transparency of practice could be communicated through disclosures, which could activate persuasion knowledge (Boerman, Willemesen, and Van Der Aa 2017) and contribute to surveillance beliefs development. Future research could investigate how to best design such disclosures and where and when to place them. Scholars could build on the sponsorship (e.g., Boerman, Willemesen, and Van Der Aa 2017) or native advertising (e.g., Wojdynski and Evans 2016) literature and extend such theories as the covert advertising recognition and effects model (Wojdynski and Evans 2020) to the digital data-driven advertising context and disclosures of data collection, processing, and sharing. Some work has already looked at disclosures in personalized advertising. For example, Van Noort, Smit, and Voorveld (2013) looked at a cookie icon that was used in the Netherlands to indicate online behavioral advertising. They found that awareness and familiarity with this icon was low and that an additional explanation was needed to correctly identify its meaning. In addition, the effect of the disclosure might depend on the trustworthiness of the source and could decrease advertising effectiveness for untrustworthy sources (Van Ooijen 2022). However, questions remain about whether and how this works for various types of data collection practices (see Segijn, Strycharz, et al. 2021 for an overview of practices with high and low transparency). From a practical perspective, studying the effectiveness of data collection disclosures will allow regulators to engage in evidence-based lawmaking and improve the implementation of current (e.g., General Data Protection Regulation) and future (e.g., Digital Services Act) regulations.

Furthermore, more research is needed to understand how to effectively inform consumers about data collection, processing, and sharing practices through education and literacy programs. Some initial studies have started to investigate different types of information on personalized communication and data collection practices and how these types of information affect consumers’ responses. For example, providing consumers with technical information on personalized communication was found to increase knowledge in people without any prior knowledge of this strategy compared to those with no information (Segijn, Kim, et al. 2021). Regarding legal knowledge, Strycharz et al. (2021) found that it improves consumers’ perceived self-efficacy when it comes to control over data collection through cookies. However, this study and one other study (Strycharz et al. 2019) found that providing people with technical information on data collection practices led to participants perceiving these practices as less severe and consequently caused participants to be less likely to use the opt-out function of data processing. Given the early stages of research into informing people about data collection for advertising purposes and mixed findings in this field, more research is needed to examine what type of information would work best to make consumers informed decision makers about their personal data.

In addition, research on developing surveillance beliefs through first- or secondhand ad exposure is needed to further understand when ad exposures contribute to and activate beliefs about data collection, processing, and sharing practices. One could argue that the more specific or more personal data are used as input to personalize a message, the more consumers may develop beliefs about how their data are used to create personalized ads for them. This would mean that exposure to more personalized ads could contribute to developing surveillance beliefs and at the same time, seeing such ads could make one think about advertisers collecting and processing their data (belief activation). More research is needed on the relationship between personalization level and surveillance beliefs, which would allow to further our theoretical
understanding of the effects of personalization on consumers and, at the same time, inform organizations that serve personalized ads about the point when an ad becomes not only persuasive but also a surveillance episode. A challenge, however, is that asking about surveillance beliefs in research itself also activates those beliefs.

**Effects of Surveillance Beliefs**

Future research should also focus on the effects of surveillance beliefs on perceived surveillance, surveillance responses, and advertising responses. Building on the transparency-awareness-control framework (Segijn, Strycharz, et al. 2021), being aware of data collection and processing results in having more control over personal data only when consumers have the ability and desire to exercise this control. Research is needed to examine the impact of surveillance beliefs on surveillance and advertising responses. But it is also important to explore consumer desire and abilities to make informed decisions based on accurate and relevant knowledge when it comes to data disclosure for advertising (as informed decision making is now one of the aims of the General Data Protection Regulation in Europe).

**Combating False Beliefs**

Finally, more research is needed into the development, activation, and combating of inaccurate beliefs, as well as the relationship to consumers’ confidence in these beliefs. Combating false beliefs and boosting confidence in accurate ones is important from the viewpoint of the industry which may suffer from disinformation about the extent of data collection and for the society as disinformation is seen as a pressing and widespread societal issue that misleads consumers and undermines trust and democracy (De Cock Bunning 2018). In addition, research is needed to further understand how folk theories relate to subsequent perceptions of surveillance and decision making (e.g., behavioral surveillance responses). Also, given that folk theories could include misinformation or conspiracy theories about how data are collected, processed, or shared, future research is needed to combat this type of misinformation, as well as the moderating role of conspiracy mentality in the relationship between perceived surveillance and advertising effects.

**Research Direction 2: Perceived Surveillance**

Future research is needed to further examine the dimensions of perceived surveillance, when it is likely to occur, and perhaps who is susceptible to it. In addition, as a second step, the relationship between perceived surveillance and surveillance and advertising responses could be examined to get a better understanding of how perceived surveillance impacts advertising effectiveness. While the negative impact of other data-collection-related factors such as privacy concerns on advertising effectiveness is known (e.g., positive impact on ad avoidance; Jung 2017), the exact role of perceived surveillance needs further investigation. Segijn et al. (2022) have validated a measurement for perceived surveillance in survey and experimental research that can facilitate this. This measurement consists of four items asking participants to rate the extent to which they feel a company/brand/person is (1) looking over your shoulder, (2) watching your every move, (3) entering your private space, and (4) checking up on you. Although this measure has been validated for personalized advertising practices specifically, it could potentially be used in other contexts as well, such as data collection through smart devices, on social media, or in stores.

Regarding prevalence of perceived surveillance, Segijn and Van Ooijen (2020) described different data collection techniques and their relation to perceived surveillance, which could serve as a starting point to examine when perceived surveillance is more likely to occur. For example, research could look at how different data collection techniques result in different levels of perceived surveillance and subsequently in surveillance and advertising responses. Studying the context in which effects of perceived surveillance are strongest will help advertisers identify the tipping point in which digital data-driven ads have unintended negative effects.

Finally, more research is needed on individual differences in susceptibility to perceived surveillance among consumers. Regarding personality, conspiracy personality that is known to contribute to awareness of data collection (Boerman and Segijn 2022) could also strengthen perceived surveillance. In the context of the surveillance effect and perceived surveillance of conversations, anxiety of new technologies and negative experiences with them are factors strongly contributing to it (Frick et al. 2021). To what extent such negative feelings and experiences drive perceived surveillance in the context of digital data-driven ads is another potential research avenue.

**Research Direction 3: Surveillance Responses**

Research is needed to examine how perceived surveillance affects cognitive, affective, and behavioral
surveillance responses. While past research has shown that benefits and costs are impacted by exposure to personalization (Bol et al. 2018), to what extent digital data-driven advertising in general changes the cost-benefit calculation requires further research. Next, while data collection is known to elicit negative emotions among consumers (Segijn and Van Ooijen 2022), to what extent these emotions are also elicited by data-driven ads remains understudied. Regarding change of behavior due to perceived surveillance, it involves taking privacy protection measures (Boerman, Kruikemeier, and Zuiderveen Borgesius 2021). However, it can also involve other behavioral adjustments aimed at limiting the extent of dataveillance and protecting personal data. Such chilling effects in response to data collection for advertising and commercial purposes remain understudied (Büchi, Festic, and Latzer 2022). Future research needs to examine what behavioral surveillance responses people undertake in reaction to data collection for advertising and what the main motivations are for undertaking such responses. What surveillance responses are elicited by exposure to digital data-driven ads will inform research and practice about potential unintended effects of digital data-driven advertising practices that go beyond traditional advertising responses.

To investigate which consumers are most likely to show surveillance responses, research on individual characteristics that contribute to these responses is needed. Boerman, Kruikemeier, and Zuiderveen Borgesius (2017) proposed a framework in which they described different consumer characteristics (e.g., privacy concerns, desire for privacy, online experience) and other consumer-controlled factors (e.g., knowledge and abilities) that could serve as a starting point for identifying consumers prone to undertaking surveillance responses. Moreover, current data collection practices are automated and continuous, constantly monitoring consumer behavior (Büchi, Festic, and Latzer 2022; Degli-Esposti 2014). This makes so-called dataveillance an important concept in the current and future advertising landscape. These new developments open new questions regarding the impact and effectiveness of advertising. The current research presents the DEAL framework and research directions designed to provide a theoretical guidance for future research on this topic. We applied long-standing theories in advertising research to this new phenomenon. A conceptualization and theorization of the role of dataveillance in the advertising landscape is crucial due to the central role consumer data play in current digital data-driven advertising and the ethical questions this centrality poses.

Beyond guiding future research on the impact of dataveillance in the advertising landscape on consumers, the DEAL framework also has practical implications for the advertising industry that applies digital data-driven advertising and for regulators who are responsible for the framework in which data collection for advertising takes place. First, for the advertising industry, the framework allows it to better understand the impact of dataveillance on consumers. This can help them anticipate the unintended effects that digital data-driven ads may have through activation of surveillance beliefs. As spillovers refer to the way in which perceptions and beliefs are affected by information that is not mentioned in the message (Ahluwalia, Unnava, and Burnkrant 2001), such spillovers could potentially explain whether perceived surveillance impacts other advertising effects. As young users already find digital advertising irrelevant, useless, and not trustworthy (Lineup 2021), the spillover effect could deepen this negative sentiment and is important for the advertising industry that tries to improve the image of digital data-driven advertising.

Second, consumer reactions to dataveillance could also impact the quality of the advertising message, which has implications for the advertising and tech industry. Following the computational advertising measurement system (Yun, Segijn, et al. 2020), data (e.g., consumer data, brand data) are used as input for advertising strategic planning and tactical execution. However, data could be polluted by consumers who provide fake information (e.g., name, e-mail address) as a privacy protection mechanism (Boerman, Kruikemeier, and Zuiderveen Borgesius 2021) or who adjust their behavior to avoid their data being collected (Büchi, Festic, and Latzer 2022). Given the
importance of data as input for computational advertising (Yun, Segijn, et al. 2020), future research is needed into the relationship between surveillance responses and data pollution. Such research could explore in what way the data are polluted and inform the industry how to prevent or account for it in algorithms.

Finally, for regulators, the framework shows how consumers form beliefs about data collection and processing practices of the industry. The description of belief formation highlights the role of transparency regulations and literacy programs in it and shows the potential regulators have in correcting false beliefs and contributing to forming correct beliefs. In addition, future research is needed to examine the DEAL framework in the context of different privacy regulations as these may impact the extent that consumers have trust in advertising companies to handle their data safely and the extent they will engage in surveillance responses. Take, for example, the difference between the United States and Europe. Privacy regulations and the amount of protection from dataveillance offered by the law differ substantially between the United States and the European Union (Tushnet and Goldman 2020). A key goal of the General Data Protection Regulation in the European Union is to strengthen individual control in the face of online data collection by corporations (Tushnet and Goldman 2020). In contrast, privacy regulations in the United States are less specific about what data on individuals can be collected, and fewer requirements have been outlined for corporations to inform users about these practices. These differences may lead to different perceptions among consumers when it comes to dataveillance (e.g., less transparency is required in the United States, resulting in less information-driven surveillance beliefs). They may also change how individuals react to surveillance episodes (e.g., one’s behavioral surveillance responses may depend on possibilities given by the law). Moreover, cross-country and cross-cultural research could help further understand the DEAL framework and the impact of dataveillance in the advertising landscape on consumers as consumer perceptions of dataveillance might depend on their cultural background and the surveillance culture where they grew up.

In addition, we identify some methodological challenges in and prerequisites for studying consumer perceptions and responses to dataveillance in advertising. For researchers who do not have access to the same data as the advertising industry does, it is difficult to measure consumer interactions with digital data-driven advertising and their surveillance and advertising. Researchers have to start using digital analytics (e.g., social media analytics; see Yun, Duff, et al. 2020) to move beyond measuring motivations and intentions (Boerman, Kruikemeier, and Zuiderveen Borgesius 2017). To access consumer data, researchers can, for example, ask consumers to donate their digital trace data (Araujo et al. 2021). This donation would make it possible to examine real-life data in relation to this topic (see Liu-Thompkins and Malthouse 2017 for a practical guide). In addition, including longitudinal designs is particularly important when it comes to perceived surveillance and surveillance responses. As the technology hype cycle shows, novel technologies move toward mainstream adoption over time (Dedehayir and Steinert 2016). This mainstream adoption changes the social norms surrounding a technology, which subsequently impacts individuals’ acceptance of it and attitudes toward it (see technology acceptance model; Davis, Bagozzi, and Warshaw 1989). When different data collection techniques for digital data-driven advertising become commonly accepted, this can possibly change consumer perceptions and responses to dataveillance.

The current article conceptualized consumer responses to dataveillance in digital data-driven advertising and applied long-standing theories in advertising research to this phenomenon. The extent of and infrastructure for data collection and processing resulting in situation of dataveillance open new questions regarding consumer responses to digital data-driven advertising. The Dataveillance Effects in Advertising Landscape framework and the proposed research directions can provide a theoretical framework to guide future research on this topic.

Note
1. See Vraga and Bode (2020) for a definition on misinformation and Swire-Thompson and Lazer (2020) for an example of misinformation in the online health misinformation context.

Acknowledgments
The authors would like to thank the editors and anonymous reviewers for their constructive input that substantially helped to shape the manuscript.

ORCID
Joanna Strycharz http://orcid.org/0000-0001-7739-3349
Claire M. Segijn http://orcid.org/0000-0002-2424-5737
References


