Computers in Human Behavior 165 (2025) 108536

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Google knows me too well! Coping with perceived surveillance in an algorithmic profiling context

Dong Zhang [a,*], Joanna Strycharz [a], Sophie C. Boerman [b], Theo Araujo [a], Hilde Voorveld [a]

[a] *Amsterdam School of Communication Research, University of Amsterdam, the Netherlands*
[b] *Strategic Communication, Wageningen University & Research, the Netherlands*

ARTICLE INFO

Handling editor: Jen-Her Wu

Keywords:
Algorithmic profiling
Perceived accuracy
Perceived surveillance
Coping strategy
Online privacy literacy
Objective accuracy

ABSTRACT

Enabled by ubiquitous dataveillance practices, corporations try to construct accurate algorithmic profiles of their users for various purposes, such as personalized advertising. In this study, we confront users with their personal algorithmic profiles and employ a cross-sectional survey ($N = 685$) to investigate how perceived accuracy of algorithmic profiling relates to perceived surveillance and subsequent coping strategies. Our findings reveal that the more accurate individuals perceive their algorithmic profiles to be, the more they feel surveilled. Subsequently, they experience more privacy cynicism, are less likely to downplay the harm of dataveillance, and have stronger intentions to adjust ad settings. Furthermore, whereas individuals with lower online privacy literacy have higher privacy cynicism regardless of their level of perceived surveillance, those with higher literacy are more likely to experience privacy cynicism as they feel more surveilled. These findings suggest that subjective evaluations of algorithmic profiling can contribute to feelings of surveillance and individual coping responses.

1. Introduction

In an era where technology permeates people's daily lives, individuals are almost inevitably subjected to the automated, continuous, and unspecific collection, storage, and processing of their digital traces (i.e., dataveillance; Büchi, Festic, & Latzer, 2022; Strycharz & Segijn, 2022). By leveraging these data, corporations can potentially create accurate algorithmic profiles of individuals. These algorithmic profiles—compilations of data referring to individuals (Büchi et al., 2020)—are used in a variety of contexts, such as advertising, content personalization, differential pricing, employment, and security (Mann & Matzner, 2019). Defined as "the systematic and purposeful recording and classification of data related to individuals" (Büchi et al., 2020, p. 2), algorithmic profiling is thus a key process enabled by—and enabling—dataveillance.

Algorithmic profiles often contain inferences regarding one's interests and sociodemographic characteristics. Whether these inferences are accurate or not may play a crucial role in how people respond to them. Observing inferences that accurately reflect themselves, individuals may be shocked by how much the company knows about them and feel unsettled (Büchi, Fosch-Villaronga, Lutz, Tamò-Larrieux, & Velidi, 2023). This suggests that when it comes to profiling, individuals may not appreciate algorithms that are overly accurate. Given the prevalence of algorithmic profiling in daily life, individuals are becoming more aware of such inferences being made (Voorveld, Meppelink, & Boerman, 2023). It is thus important to deepen our understanding of the impact of algorithmic profiling, specifically focusing on the role of perceived accuracy, that is, how accurately users perceive their algorithmic profiles to reflect themselves.

A growing body of research indicates that observing or being aware of data collection induces perceived surveillance—the feeling of being surveilled (e.g., Segijn & van Ooijen, 2020; Sifaoui, Lee, & Segijn, 2023; Strycharz & Segijn, 2022). Since previous research has shown that people easily comprehend that profiling inferences are drawn based on their personal data (Büchi et al., 2023), they might perceive surveillance from the company creating these algorithmic profiles. Previous literature examining the consequences of perceived surveillance mainly focused on its impact on advertising effectiveness (e.g., Segijn, Kim, Sifaoui, & Boerman, 2023; Segijn & van Ooijen, 2020; Sifaoui et al., 2023). However, according to the reactance theory, individuals might also feel compelled to *cope* with it as they might perceive it as a threat to their freedom (Brehm & Brehm, 1981; Segijn, Kim, Lee, Gansen, &

[*] Corresponding author. Amsterdam School of Communication Research, Postbus 15791, 1001 NG, Amsterdam, the Netherlands.
E-mail address: d.zhang@uva.nl (D. Zhang).

https://doi.org/10.1016/j.chb.2024.108536
Received 22 April 2024; Received in revised form 6 December 2024; Accepted 7 December 2024
Available online 10 December 2024

Boerman, 2023). Existing studies have identified several strategies individuals use to cope with the discomfort brought by dataveillance: privacy cynicism (an attitude of uncertainty, powerlessness, mistrust, and resignation regarding one's online privacy; Lutz, Hoffmann, & Ranzini, 2020), self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation (Marwick & Hargittai, 2019; Zhang et al., 2024). Moreover, perceived surveillance may also trigger privacy-protection behaviors (Strycharz & Segijn, 2022). Therefore, the first aim of this study is to investigate how perceived accuracy of algorithmic profiling relates to perceived surveillance, and subsequently, how people cope with perceived surveillance through privacy protection behavior intention and four cognitive strategies.

Prior research has shown that internet users with higher online privacy literacy are not only more capable of protecting themselves through privacy-protection behaviors (Bartsch & Dienlin, 2016; Baruh, Secinti, & Cemalcilar, 2017; Park, 2013) but also possess more agency to achieve their own online goals (Masur, 2020). Hence, to account for potential individual differences, the second aim of the study is to examine the moderating role of online privacy literacy on the relationship between perceived surveillance and coping. By doing so, we broaden the currently limited literature on the boundary conditions of perceived surveillance.

Additionally, while this study focuses on the role of perceived accuracy of algorithmic profiling, most research in algorithmic system development employs objective accuracy (how well the algorithm actually predicts user characteristics and interests) for performance evaluation (Eke, Norman, Shuib, & Nweke, 2019). However, evidence is mixed regarding whether the two constructs are related to each other and which one more directly influences individual responses (Pu, Chen, & Hu, 2012). Thus, the third aim of this study is to explore how perceived accuracy relates to objective accuracy of algorithmic profiling and how the latter relates to perceived surveillance and coping.

This study makes several contributions to the current literature: First, we advance the knowledge about how individuals respond to algorithmic profiling, specifically to perceived and objective accuracy of algorithmic profiling. Second, we extend the context of research on perceived surveillance to algorithmic profiling and examine its relationship with individual coping rather than advertising effectiveness. Third, alongside privacy-protection behavioral intention, we incorporate and differentiate between four cognitive coping strategies, some of which have yet to be quantitatively examined in previous research. Fourth, we explore the conditional roles of online privacy literacy, which informs theory advancement on how individual differences might affect a surveillance response process. To examine the aforementioned relationships, we guided individuals to view their own algorithmic profiles in real life and captured their immediate responses. This approach provided a genuine dataveillance experience involving users' own data, thereby ensuring the ecological validity of our findings.

In sum, the main aim of the current study is to investigate to what extent perceived accuracy of algorithmic profiling relates to individuals' perceived surveillance and subsequent coping responses (i.e., privacy protection behavioral intention, privacy cynicism, self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation). Additionally, we explore how individuals with varying levels of online privacy literacy cope differently and how perceived accuracy relates to the objective accuracy of algorithmic profiling.

2. Theoretical framework

2.1. Perceived accuracy and perceived surveillance

Given that an algorithmic profile is "a compilation of data referring to an individual" (Büchi et al., 2020, p. 2), *perceived accuracy* of algorithmic profiling can be defined as the extent to which users perceive the algorithmic profile to reflect themselves as individuals. Past research on individual responses toward algorithmic profiling has briefly touched upon perceived accuracy: Although individuals expect algorithmic profiling to be accurate and feel surprised by inaccurate inferences (Eslami, Krishna Kumaran, Sandvig, & Karahalios, 2018, pp. 1–13; Hautea, Munasinghe, & Rader, 2020), highly accurate inferences simultaneously make them feel uncomfortable and are perceived as a threat to their agency (Büchi et al., 2023; Grill & Andalibi, 2022; Rader, Hautea, & Munasinghe, 2020, pp. 457–488). However, it is unclear through what mechanism high perceived accuracy triggers this discomfort.

The theory of psychological ownership suggests that individuals can feel that they are in possession of intangible targets, including digital data, irrespective of the legal ownership (Cichy, Salge, & Kohli, 2014; Pierce, Kostova, & Dirks, 2003). Psychological ownership emerges when one feels familiar, associated with, or has intimate knowledge of the target (van Dijk & van Knippenberg, 2005). When it comes to algorithmic profiling, the more accurate the inference (e.g., a predicted interest matches one's actual interest), the more intimate and knowledgeable one may feel toward this piece of information, and the stronger the sense of ownership. In that case, realizing the company also knows this information might raise the feeling of being surveilled (Segijn, Kim, Sifaoui, & Boerman, 2023).

According to the dataveillance effects in advertising landscape (DEAL) framework (Strycharz & Segijn, 2022), a directly observable instance of data collection (i.e., a surveillance episode) may trigger *perceived surveillance*—the feeling of being watched, listened to, or that one's personal data are being recorded (Segijn, Opree, & Ooijen, 2022). The most prevalent surveillance episodes occur when individuals encounter personalized advertising or content in the digital environment, where algorithmic profiling serves as a crucial mechanism for generating such content (Zhang, Boerman, Hendriks, Araujo, & Voorveld, 2023, 2024). As such, directly inspecting one's own algorithmic profile could make data collection even more evident, as users are confronted with an extensive list of inferences that are explicitly stated to be based on their online behavior (Büchi et al., 2023; Rader et al., 2020, pp. 457–488). Büchi et al. (2022) further 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 specifics of a surveillance episode may determine the strength of its impact on perceived surveillance. Sifaoui (2021) found that advertising with higher levels of personalization (ads containing matching versus non-matching brands with search history) increases perceived surveillance. In line with this, we postulate that algorithmic profiling that is perceived to be more accurate could trigger stronger perceived surveillance, leading to the following hypothesis.

H1. The perceived accuracy of algorithmic profiling is positively related to perceived surveillance among individuals.

2.2. Coping with perceived surveillance

Since individuals could feel surveilled due to seeing highly accurate algorithmic profiles, they may feel the need to cope with this unpleasant feeling. Feeling surveilled means that the person is aware of the ongoing dataveillance practice and perceives a threat to their freedom of determining what the company can or cannot know about themself (Farman, Comello, Nori, & Edwards, 2020). Psychological reactance theory suggests that those who experience a threat to their control or freedom are motivated to resist such influence to restore their freedom (Brehm & Brehm, 1981). Therefore, increased feelings of surveillance may lead to greater psychological reactance and stronger motivation to cope with such feelings (Farman et al., 2020).

Existing studies on perceived surveillance focused on its effects on consumers' reactance to advertising: perceived surveillance is reported to induce ad avoidance (Sifaoui et al., 2023), ad contesting (Segijn, Kim, Sifaoui, & Boerman, 2023), and less acceptance of personalization techniques (Segijn & van Ooijen, 2020). While an algorithmic profile itself is not a persuasive attempt that can be avoided, contested, or rejected, individuals may still be motivated by the threat to their freedom to go through a similar reactance process. Previous research has identified a number of coping strategies individuals employ in response to perceived surveillance (e.g., Strycharz, Kim, & Segijn, 2022; Strycharz & Segijn, 2022; Zhang et al., 2024). In this study, we examine five strategies that were observed across multiple studies: privacy protection behavioral intention, privacy cynicism, self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation. These coping strategies correspond with five established resistance strategies in the persuasion literature: avoidance, inertia, biased processing, empowerment, and contesting (Fransen, Smit, & Verlegh, 2015; Knowles & Linn, 2004). Below, we elaborate on how these coping strategies align with the resistance strategies and how they are applied by individuals in a digital dataveillance context.

2.2.1. *Privacy protection behavioral intention*

As a measure to reduce the collection, processing, and sharing of personal information, privacy protection behavior serves as an avoidance strategy (Fransen et al., 2015; Strycharz & Segijn, 2022). The greater the perceived threat, the more likely people will engage in privacy protection behavior (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2021; Meier, Schäwel, Kyewski, & C. Krämer, 2020). When confronted with one's algorithmic profile, the most probable privacy protection behavior is adjusting the ad personalization settings on the platform, as these settings are typically easily accessible within the page containing the profile and can directly alter the profile. Individuals perceiving higher levels of surveillance would be more motivated to restore their freedom, and thus more inclined to adjust their ad settings.

2.2.2. *Privacy cynicism*

When one is unable or chooses not to take actions to reduce dataveillance, they might cope with perceived surveillance on a cognitive level. Privacy cynicism, a coping mechanism particular to the digital context, refers to an attitude of uncertainty, powerlessness, and mistrust toward the handling of personal data by digital platforms and the subjective belief that privacy protection efforts are futile (Hoffmann, Lutz, & Ranzini, 2016; Lutz et al., 2020). This mirrors the inertia facet of resistance (Knowles & Linn, 2004), which emphasizes staying put rather than resisting change. Zhang et al. (2024) and Kappeler, Festic, and Latzer (2023) both observed that despite a prevalent feeling of surveillance, many individuals believe there is little they can do to protect themselves, which is captured by privacy cynicism.

2.2.3. *Self-empowerment*

Contrastingly, some individuals empower themselves by thinking of the benefits of being under dataveillance and reaffirming their control (Strycharz et al., 2022; Zhang et al., 2024). This echoes the empowerment resistance strategy as it focuses on strengthening one's existing attitudes and asserting self-confidence (Fransen et al., 2015). Individuals experience numerous benefits brought by dataveillance, such as personalization (Jung, 2017), convenience (Lau, Zimmerman, & Schaub, 2018), and usefulness (Ur, Leon, Cranor, Shay, & Wang, 2012, pp. 1–15). When feeling surveilled, people may remind themselves of these benefits to reduce the psychological reactance while maintaining the status quo.

2.2.4. *Downplaying dataveillance cost*

Another strategy involves downplaying the cost of dataveillance by diminishing the perceived threat with arguments like "nothing to hide, nothing to lose" (Marwick & Hargittai, 2019). Individuals claim they see no harm or threat as a reason not to change their media use in response to perceived surveillance (Strycharz et al., 2022). By downplaying the cost of dataveillance, individuals attribute less weight to information that elicits perceived surveillance, akin to the biased processing strategy to resist persuasion (Fransen et al., 2015).

2.2.5. *Sympathizing with the corporation*

Finally, people may sympathize with the dataveillance source by taking the perspective of the corporations, as they understand why corporations engage in algorithmic profiling (e.g., to generate revenue to continue providing free services) (Zhang et al., 2024). This can be seen as the opposite of source contesting (Fransen et al., 2015), as individuals who use this strategy actively support the stance of the corporation. This is similar to the phenomenon that YouTube users intentionally view skippable ads to support video creators (Kim & Huh, 2023), since in both cases users show an understanding of the revenue model of the digital product and are willing to reciprocate the benefits they have received.

Aligned with our proposition that people who experience more perceived surveillance are more likely to engage in coping, we hypothesize.

H2. Perceived surveillance is positively associated with (a) intention to adjust ad settings, (b) privacy cynicism, (c) self-empowerment, (d) downplaying dataveillance cost, and (e) sympathizing with the corporation.

As we expect higher perceived accuracy of algorithmic profiling leads to stronger perceived surveillance and perceived surveillance increases coping, perceived surveillance should play a mediating role between perceived accuracy and coping. The hypothesis is as follows.

H3. Perceived surveillance positively mediates the positive relationships between perceived accuracy of algorithmic profiling and (a) intention to adjust ad settings, (b) privacy cynicism, (c) self-empowerment, (d) downplaying dataveillance cost, and (e) sympathizing with the corporation.

2.3. *The role of online privacy literacy*

Individual traits may drive different reactions to perceived surveillance (Strycharz & Segijn, 2022). One such trait is online privacy literacy, which is a combination of factual privacy knowledge, privacy-related reflection abilities, privacy and data protection skills, and critical privacy literacy (Masur, Hagendorff, & Trepte, 2023). Past works have established that internet users with higher online privacy literacy are more capable of adopting privacy protection behaviors (Bartsch & Dienlin, 2016; Baruh et al., 2017; Park, 2013). Kappeler et al. (2023) observed that individuals with more internet skills tend to counter perceived surveillance more with privacy protection techniques. Furthermore, Masur (2020) argues that besides privacy protection, online privacy literacy also enables informational self-determination, meaning that high-literacy individuals have more agency and ability to decide when and how personal information should be collected, analyzed, or communicated, depending on their own goals. Stubenvoll and Binder (2024) found that users with higher privacy literacy perceive higher self-efficacy. For these individuals, perceived surveillance might motivate them to support their current stance with self-empowering thoughts.

Following this argument, we postulate that having high literacy gives users the agency to approach and address the psychological threat when feeling surveilled, either by intending to adjust ad settings or self-empowerment. Conversely, for users with lower levels of literacy, due to their lack of agency, perceived surveillance is more likely to lead to privacy cynicism as a passive way of coping to avoid cognitive dissonance (Hoffmann et al., 2016). Individuals with lower literacy are also less capable of assessing the privacy risks of different online environments (Masur, 2020), thus more likely to downplay the cost of dataveillance when feeling surveilled.

Additionally, we explore whether and how online privacy literacy moderates the relationship between perceived surveillance and sympathizing with the corporation. According to Masur (2020), one sub-dimension of online privacy literacy is knowledge about economic interests and data collection, analysis, and sharing practices of online service providers. Therefore, highly skilled internet users might have a better understanding of the economic motives of algorithmic profiling for corporations, which means online privacy literacy could positively moderate the relationship between perceived surveillance and sympathizing. However, current evidence is too limited for a hypothesis.

Based on these arguments, we investigate the moderating role of online privacy literacy on the relationship between perceived surveillance and coping.

H4. Online privacy literacy strengthens the relationships between perceived surveillance and (a) intention to adjust ad settings and (c) self-empowerment, but weakens the relationships between perceived surveillance and (b) privacy cynicism and (d) downplaying dataveillance cost.

RQ1. To what extent does online privacy literacy moderate the relationship between perceived surveillance and sympathizing with the corporation?

2.4. *Perceived accuracy and objective accuracy*

As defined earlier, perceived accuracy is a user's subjective evaluation of how much the profile reflects themself as an individual. This is distinct from the objective accuracy of the algorithmic profiles—the extent to which the algorithm correctly predicts the actual traits and interests of the individual being profiled. While acquiring perceived accuracy relies fully on the user's assessment after personally inspecting the profile, objective accuracy can technically be calculated by comparing the inferences with a list of traits and interests from the user without the user evaluating the algorithmic profile themself.

It is logical to assume that perceived accuracy is related to the objective accuracy of the algorithm. Research has found a correlation between perceived and objective accuracy for classification algorithms (Fairclough, Karran, & Gilleade, 2015, pp. 3029–3038). However, this assumption might not hold true for user profiling algorithms, as users may perceive certain inferences that are generated based on their actual online behavior to be inaccurate, or they might find justification for an objectively inaccurate result to be accurately describing themselves, making the relationship inconclusive (Barbosa, Wang, Ur, & Wang, 2021; Eslami et al., 2018, pp. 1–13).

Furthermore, research suggests that perceived accuracy has a more direct influence on user trust and behavioral intentions (L. Chen & Pu, 2009). Indeed, in studies where individuals reported feeling uncomfortable with accurate algorithmic profiles, the accuracy was judged subjectively by the individuals themselves (e.g., Büchi et al., 2023; Hautea et al., 2020; Rader et al., 2020, pp. 457–488). Nevertheless, there is no research explicitly comparing perceived and objective accuracy in an algorithmic profiling setting.

However, learning from research on actual versus perceived personalization (Li, 2016) and interactivity (Voorveld, Neijens, & Smit, 2011), there seems to be a distinction as well as a connection between the objective quality of a technical system and the subjective evaluation of this particular quality by individuals. Designing a message based on information about an individual makes it factually personalized, while the message receiver may not perceive it to be personalized (Li, 2016). Similarly, adding more interactive features to a website does not guarantee higher perceptions of interactivity (Voorveld et al., 2011). These studies suggest that there could be an incongruence between perceived and objective accuracy, and perceived accuracy may have a stronger and more direct link to individual responses. We therefore explore whether perceived and objective accuracy are related to each other, and the relationship between objective accuracy, perceived surveillance, and coping strategies.

RQ2. To what extent does objective accuracy of algorithmic profiling relate to perceived accuracy of algorithmic profiling?

RQ3. How does objective accuracy of algorithmic profiling relate to perceived surveillance?

RQ4. How does objective accuracy of algorithmic profiling through perceived surveillance indirectly relate to (a) intention to adjust ad settings, (b) privacy cynicism, (c) self-empowerment, (d) downplaying dataveillance cost, and (e) sympathizing with the corporation?

The conceptual model is visualized in Fig. 1.

3. Methods

3.1. *Design and sample*

In this study, we conducted a survey in which we guided participants in viewing the actual algorithmic profiles that belonged to themselves and inquired about their reactions immediately afterward. To individual users, algorithmic profiling has been an opaque process with little information about its inner workings disclosed (Eslami et al., 2018, pp. 1–13; Pasquale, 2015). However, in the past years, several major technological platforms have made the algorithmic profiles they use for ad personalization accessible to users (Google, n.d.; Meta, n.d.). We chose to ask participants to review their algorithmic profiles from Google for its broad user base and its comprehensive algorithmic profile that is easily accessible via a site called Google My Ad Center, which showed inferred interests ("topics") and inferred sociodemographic categories on two separate pages (Google, n.d.; Similarweb, n.d.).

This study was approved by the Ethics Review Board and Data Stewards at the first author's institute (project reference number: FMG-6435) and has been pre-registered on the Open Science Framework (OSF).[1] The data were collected in February 2024 via Prolific, using a quota sample mirroring the age and sex distribution of the adult population in the United Kingdom (UK). Eligible participants were required to have owned Google accounts (eligibility rate = 99.7%), used their accounts the previous month (eligibility rate = 99.0%), and had their Google ad personalization setting turned on at the time of participation (eligibility rate = 75.0%), as the algorithmic profile was only visible to users with the setting turned on.[2] Four participants were excluded for failing both attention checks, and six participants were excluded for not recommending the use of their responses in the research. The final sample (N = 685) had an average age of 45.5 years (SD = 15.2). The sample characteristics regarding gender, education, Google services use frequency, and prior visit to Google My Ad Center are shown in Table 1.

3.2. *Pretest*

A pretest (registered and approved as [PROJECT NUMBER REMOVED FOR PEER REVIEW] at the institute) was conducted among 57 university students to ensure that there was sufficient variance in the level of perceived accuracy based on the Google algorithmic profile to examine the subsequent relationships. Pretest participants were recruited from the online laboratory of the first author's university. After providing informed consent, participants visited their Google My Ad Center and separately rated the perceived accuracy of inferred sociodemographic information (M = 6.37, SD = 2.65) and inferred interests (M = 6.60, SD = 1.99). For both types of inferences, the perceived accuracy was moderate with substantial variances. We also learned that a significant percentage of participants (n = 27, 47.4%) could not access

[1] https://osf.io/at4eg

[2] We inquired the demographic information from people who had previously turned off Google ad personalization. Compared to eligible participants, these respondents were on average three years older (M = 48.5, SD = 15.7), t (445.98) = 2.57, p = .010, but did not differ in gender or education distribution. A larger proportion (33.9%) had visited Google My Ad Center before, χ^2 (2, N = 942) = 38.00, p < .001.

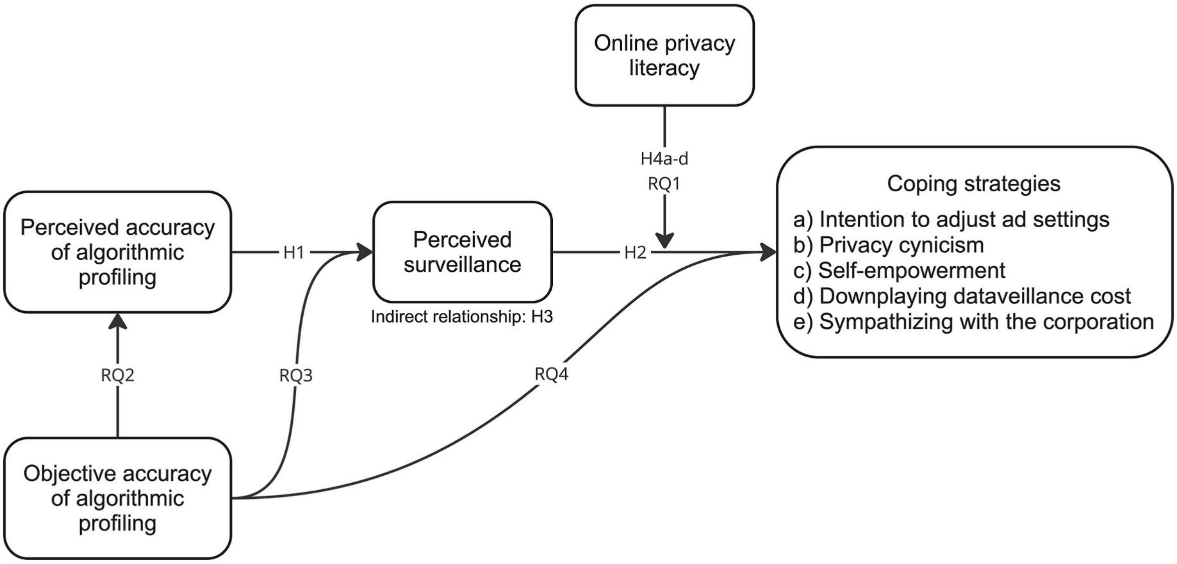
Online privacy literacy
H4a-d
RQ1
Coping strategies
a) Intention to adjust ad settings
b) Privacy cynicism
c) Self-empowerment
d) Downplaying dataveillance cost
e) Sympathizing with the corporation
Perceived accuracy of algorithmic profiling
H1
Perceived surveillance
H2
Indirect relationship: H3
RQ2
RQ3
RQ4
Objective accuracy of algorithmic profiling

Fig. 1. Conceptual model.

Table 1
Sample characteristics.

Characteristics	*n*	%
Gender		
Female	348	50.8
Male	333	48.6
Non-binary/others	3	0.4
Prefer not to say	1	0.1
Education		
Primary or lower secondary education	88	12.8
Upper secondary/further education	137	20.0
Undergraduate education	310	45.3
Postgraduate education	150	21.9
Google services use frequency		
Once a month	3	0.4
A few times a month	11	1.6
Once a week	9	1.3
Multiple times a week	52	7.6
Once a day	31	4.5
Multiple times a day	579	84.5
Prior visit to Google My Ad Center		
No	416	60.7
No, but have heard of it	162	23.6
Yes	107	15.6

the algorithmic profiles because they turned off the ad personalization feature in their Google accounts, so we could anticipate recruiting a larger sample and check for potential biases between eligible versus non-eligible respondents in the main survey.

3.3. Procedure

In the main survey, upon giving informed consent, respondents were first screened on their Google account ownership, use, and current ad personalization setting. Participants were then instructed to inspect the inferred interests and sociodemographic categories in their Google My Ad Center. Specifically, we instructed participants to focus on two areas on the website: “Topics” under the page “Customize Ads”, which were the inferred interests, and “Categories used to show you ads” under the page “Manage Privacy”, which were the inferred sociodemographic categories (see the instructional screenshots used in the questionnaire on OSF).[3] Afterward, they responded to the measures of perceived accuracy of algorithmic profiling, perceived surveillance, and the five coping strategies. Next, participants were asked to copy and paste the text content of both pages they visited in their Google My Ad Center—one containing inferred interests and one containing inferred sociodemographic categories—and answered questions for computing the objective accuracy of each page. We reassured participants that the data regarding their inferred and actual sociographic information and interests would only be used to compute the accuracy of the inferences with guaranteed anonymity.[4] Lastly, we measured participants’ online privacy literacy, potential covariates (prior attitude towards personalized advertising on Google, need for privacy, and internet privacy concerns), and demographic information.

3.4. Measures

The measurement items, sources, descriptive statistics, and reliability scores of all scale measures can be found in Table 2. A correlation matrix of all continuous variables is available on OSF under “Correlation matrix”.[5]

Perceived accuracy of algorithmic *profiling* was measured with five items, inspired by the single-item measurement from Büchi et al. (2023) and further expanded by the authors. We asked participants how accurately they thought the inferences reflected their lifestyle, preferences, needs and wishes, personal characteristics, and them as a person. *Perceived surveillance* was measured with four items by Segijn et al. (2022). *Online privacy literacy* was assessed using four items by Piotrowski, Vries, and Vreese (2021).

Regarding the coping strategies, the questions were led with the statement “after seeing the inferences Google made about me …” with the aim of establishing causal links between seeing the algorithmic profiles and coping. *Intention to adjust ad settings* was measured by asking participants how likely they would change each of the three possible settings on Google My Ad Center, such as limiting the types of data

[3] https://osf.io/gf6ze

[4] To protect participants’ anonymity, these data are not included in the published dataset. To replicate our measures of objective accuracy, one can use the calculated scores of the sociodemographic inferences and the indicated levels of interests in the dataset (see Measures – Objective accuracy of algorithmic profiling).

[5] https://osf.io/d56fu

Table 2
Measurement items, descriptive statistics, and reliability scores.

Measurement items	*M*	*SD*	Cronbach's alpha
Perceived accuracy of algorithmic profiling (inspired by Büchi et al., 2023)			
Looking at the inferences made by Google on both pages, how accurately would you say they reflect … (0 = *not at all accurately*; 10 = *extremely accurately*)	5.10	2.07	0.94
• Your lifestyle			
• Your preferences			
• Your needs and wishes			
• Your personal characteristics			
• You as a person			
Perceived surveillance (Segijn et al., 2022)			
When seeing the inferences Google made about me, I felt that Google was … (1 = *not at all*; 7 = *very much*)	4.07	1.63	0.94
• Watching my every move			
• Checking up on me			
• Looking over my shoulder			
• Entering my private space			
Intention to adjust ad settings (items aligned with setting options provided in Google My Ad Center)			
After seeing the inferences Google made about you, how likely would you … (1 = *very unlikely*; 7 = *very likely*)	4.38	1.62	0.90
• Disable certain categories/topics that Google can use for personalized ads (e.g., disallow Google from using relationship status to personalise ads)			
• Limit the types of data Google can use to generate personalized ads (e.g., disallow Google from using your search history, browsing history, or location history for personalizes ads)			
• Turn off ad personalization on Google			
Privacy cynicism (Lutz et al., 2020)			
After seeing the inferences Google made about me, I felt that … (1 = *strongly disagree*; 7 = *strongly agree*)	3.40	1.25	0.87
• There is no point in dedicating too much attention to the protection of my personal data online			
• I can't be bothered to spend much time on data protection on the Internet			
• I have given up trying to keep up-to-date with current solutions for protecting my personal data online			
• I am careless with my personal data online because it is impossible to protect them effectively			
• It doesn't make a difference whether I try to protect my personal data online or not			
Self-empowerment (Briñol et al., 2004)			
When seeing the inferences Google made about me … (1 = *extremely unlike me*; 7 = *extremely like me*)	3.81	1.17	0.91
• I remind myself why being able to use Google is important to me			
• I would like to make a mental list of the reasons in support of using Google			
• I would like to think about why using Google is right for me			
• I try to think about things that support the attitude I already have about Google			
• I think it's good to think about my values and beliefs regarding my usage of Google			
• I think of all the reasons in support of using Google			
Downplaying dataveillance cost (Strycharz et al., 2022)			
After seeing the inferences Google made about me, I thought … (1 = *not at all*; 7 = *very much*)	4.10	1.30	0.91
• I do not see any potential harm of Google making these inferences about me			
• I do not believe my information will be abused by Google			
• I do not see potential threats of Google making these inferences about me			
• It does not bother me that Google makes these inferences about me			
• I do not care about Google making these inferences about me			
• I have nothing to hide from Google			
Sympathizing with the corporation (inspired by Davis, 1980; Zhang et al., 2024)			
After seeing the inferences Google made about me … (1 = *not at all*; 7 = *very much*)	4.27	1.36	0.90
• I put myself in Google's shoes to understand why it makes inferences about its users			
• I take Google's perspective to understand why it collects data from its users			
• I see things from Google's point of view to understand why it wants information about its users			
• I tend to imagine that if I was Google, I would also try to figure out what the users are like			
Objective accuracy of algorithmic profiling - sociodemographic inferences (items and answer options aligned with inferences categories and options in Google My Ad Center)			
Categories that were inferred and measured included:	0.42	0.24	
• Relationships			
• Education			
• Industry			
• Employer size			
• Homeownership			
• Parenting			
The final score indicates the percentage of correctly inferred categories out of all answered categories by each participant.			
Objective accuracy of algorithmic profiling - interest inferences (Bashir, Farooq, Shahid, Zaffar, & Wilson, 2019)			
For each of the 10 randomly selected inferred interests: To what extent are you interested in the following topics? (1 = *not at all interested*; 7 = *very much interested*)	4.18	1.15	
Online privacy literacy (Piotrowski et al., 2021)			
To what extent do you think the following statements apply to you? (1 = *completely untrue*; 7 = *completely true*)	5.54	0.97	0.74
• I know how to adjust the privacy settings on a mobile phone or tablet			
• I know how to change the location settings on a mobile phone or tablet			
• I know how to identify suspicious email messages that try to get my personal data			
• I know how to delete the history of websites that I have visited before			
Prior attitude towards personalized advertising on Google (Pollay & Mittal, 1993)			
Prior to participating in this study, …(1 = *strongly disagree*; 7 = *strongly agree*)	4.07	1.37	0.94
• I considered that seeing personalized ads on Google services was a good thing			
• My general opinion of seeing personalized ads on Google services was favorable			
• I liked seeing personalized ads on Google services			

(*continued on next page*)

Table 2 (*continued*)

Measurement items	*M*	*SD*	Cronbach's alpha
*Need for privacy (*Frener et al., 2023*)*			
In general, to what extent do you agree or disagree with the following statements? (1 = *I do not agree at all*; 7 = *I entirely agree*)	5.76	0.97	0.86
• I would prefer that little is known about me			
• In general, I prefer to remain unknown			
• I do not want my personal data to be publicly accessible			
• Not everyone has to know everything about me			
*Internet privacy concerns (*Dinev & Hart, 2006*)*			
In general, to what extent are you concerned or not concerned about the following? (1 = *not at all concerned*; 7 = *very concerned*)	5.21	1.34	0.94
• I am concerned that the information I submit on the Internet could be misused			
• I am concerned that a person can find private information about me on the Internet			
• I am concerned about submitting information on the Internet, because of what others might do with it			
• I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee			
*Privacy invasion experience (*Bansal et al., 2010*)*			
When it comes to the privacy invasion of my personal data, my online experience could be characterized as:	2.96	1.44	0.91
• Never victimized (1) – Definitely victimized (7)			
• No bad experiences (1) – A lot of bad experiences (7)			
• No invasion of privacy at all (1) – A great deal of invasion of privacy (7)			

Google can use to generate personalized ads. *Privacy cynicism* was measured with five items from the resignation dimension of privacy cynicism, which was the most state-like dimension rather than a trait (Lutz et al., 2020). *Self-empowerment* was measured with six items by Briñol, Rucker, Tormala, and Petty (2004). *Downplaying dataveillance cost* was measured with six items from Strycharz et al. (2022). *Sympathizing with the corporation* was measured with four self-developed items inspired by Zhang et al. (2024) and Davis (1980).

Objective accuracy of algorithmic profiling was measured with two separate indicators: *objective accuracy of sociodemographic inferences* and *objective accuracy of interest inferences*. The reason for having two separate indicators was that while the actual sociodemographic categories can be reported by individuals with a high level of certainty, it is not equally easy for a participant to judge whether a topic is considered as their "true" interest or not. Therefore, we computed binary scores for each sociodemographic category but measured the objective accuracy of interest inferences with an ordinal scale. For *sociodemographic inferences*, we extracted the inferred categories from the uploaded page content and compared them with participants' self-reported situation for each sociodemographic category ($n = 636$). We then calculated a score between 0 and 1, which indicates the percentage of correctly inferred categories out of all the available categories answered by participants.[6] For *interest inferences*, once participants uploaded their page content, the questionnaire was programmed to parse the textual input and randomly extract 10 inferred interests to be displayed on the next page ($n = 683$). Participants then indicated the extent to which they were interested in each topic. We then computed the mean score of all indicated interest levels to form a score between 1 and 7.[7]

Additionally, we measured four potential covariates as previous studies showed that they might be related to either perceived surveillance or one of the coping strategies.[8] *Prior attitude towards personalized advertising on Google* was measured with three items (Pollay & Mittal, 1993). The personality trait *need for privacy* was measured with four items by Frener, Dombrowski, and Trepte (2023). *Internet privacy concerns* were measured using four items from Dinev and Hart (2006). Lastly, participants rated their *privacy invasion experience* on three semantic differential items (Bansal, Zahedi, Mariam, & Gefen, 2010).

3.5. Data analysis

We tested H1-H4, RQ1, RQ3, and RQ4 with model 14 of the PROCESS macro using 5000 bootstrap samples (Hayes, 2022). For H1-H4 and RQ1, five moderated mediation models were estimated, with perceived accuracy of algorithmic profiling serving as the independent variable, perceived surveillance as the mediator, online privacy literacy as the moderator, and each of the five coping strategies as the dependent variable for each analysis. For RQ3 and RQ4, the models contained objective accuracy of algorithmic profiling for sociodemographic inferences and for interest inferences as the independent variables separately instead. Covariates were included based on the four criteria recommended by Meyvis and van Osselaer (2018) for each dependent variable.[9] For RQ2, we conducted a correlation analysis between perceived accuracy and the two indicators of objective accuracy. Additionally, we conducted linear regression analyses with only perceived accuracy and covariates in the model to estimate the total effects of perceived accuracy on each coping strategy. The data analyses were conducted in R with the code available on OSF under "Data analysis".[10]

4. Results

4.1. Perceived accuracy, perceived surveillance, and coping

We first tested the relationship between perceived accuracy of algorithmic profiling and perceived surveillance (H1). In line with H1, perceived accuracy was positively related to perceived surveillance: the more accurate one perceived their algorithmic profile to be, the more likely they felt surveilled by Google, $b^* = 0.31$, $p < .001$, 95% CI [0.24, 0.37].

H2 investigated the relationships between perceived surveillance and the five coping strategies. Perceived surveillance had positive relationships with intention to adjust ad settings ($b^* = 0.32$, $p < .001$, 95% CI [0.25, 0.39]) and privacy cynicism ($b^* = 0.09$, $p = .024$, 95% CI [0.01, 0.18]), supporting H2a and H2b. Quite paradoxically, this means that people who felt surveilled by Google were not only more likely to adjust their ad settings, but also more likely to feel that privacy protections are futile. Perceived surveillance was not related to self-empowerment ($b^* = 0.03$, $p = .479$, 95% CI [−0.05, 0.10]) and

[6] For most participants ($n = 457$), the composite score was calculated based on all six categories in Google My Ad Center: relationship status, education, industry, employer size, home ownership, and parenting situation. However, some participants ($n = 179$) have turned off certain categories in their profiles or did not answer the questions to their actual situations of certain categories. In these cases, the composite scores were calculated based on the categories available.

[7] The exact instructions for both objective accuracy measures can be found on OSF under "Measurement statistics" (https://osf.io/yx2ac).

[8] The justifications for the inclusion of the potential covariates are available on OSF under "Covariate inclusion" (https://osf.io/rqhmx).

[9] See OSF "Covariate inclusion" for details (https://osf.io/rqhmx).

[10] https://osf.io/dkx38

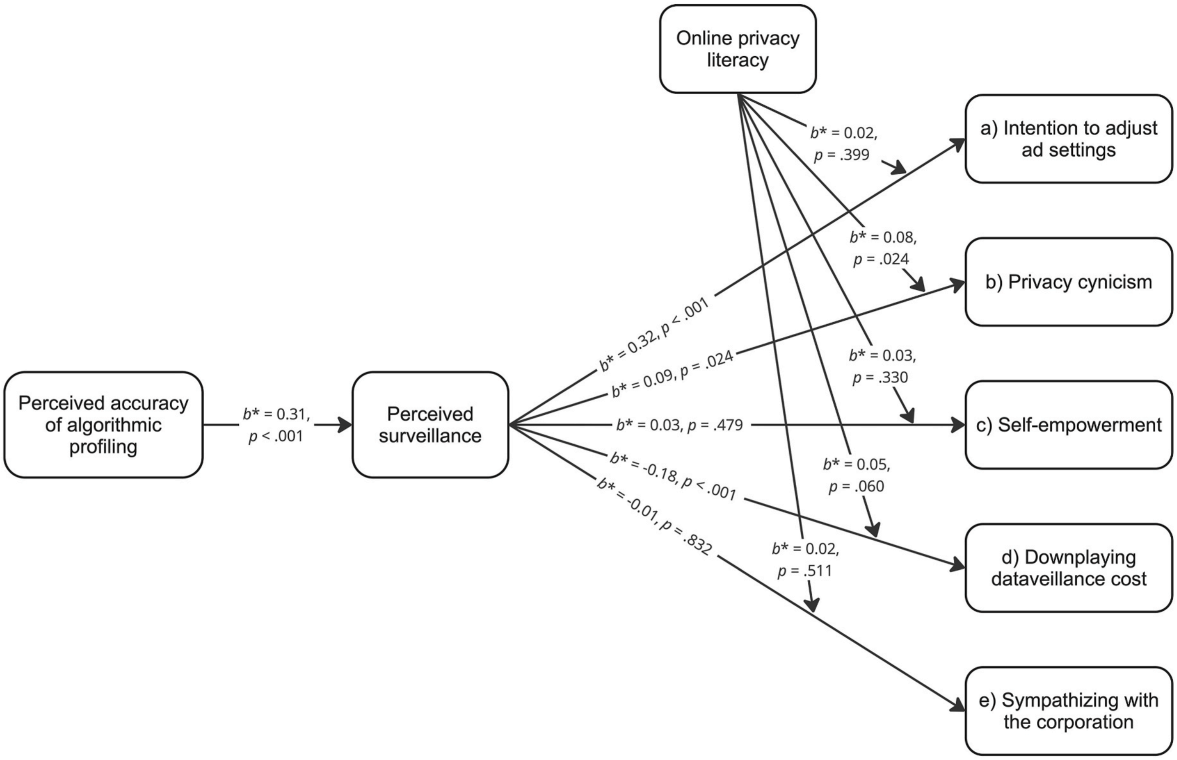

Fig. 2. Relationships between perceived accuracy, perceived surveillance, online privacy literacy, and coping strategies.

Table 3
Indirect, direct, and total relationships of perceived accuracy through perceived surveillance on coping strategies.

Path	*b**	(Boot) *SE*	95% (Boot) CI
a) Intention to adjust ad settings			
Indirect	**0.10**	**0.02**	**[0.07, 0.13]**
Direct	**−0.11**	**0.03**	**[-0.18, -0.04]**
Total	0.01	0.03	[-0.06, 0.07]
b) Privacy cynicism			
Indirect	**0.03**	**0.01**	**[0.00, 0.06]**
Direct	0.06	0.04	[-0.02, 0.13]
Total	**0.08**	**0.04**	**[0.00, 0.15]**
c) Self-empowerment			
Indirect	0.01	0.01	[-0.02, 0.03]
Direct	**0.35**	**0.04**	**[0.28, 0.42]**
Total	**0.36**	**0.04**	**[0.28, 0.43]**
d) Downplaying dataveillance cost			
Indirect	**−0.06**	**0.01**	**[-0.08, -0.03]**
Direct	**0.10**	**0.03**	**[0.04, 0.16]**
Total	0.04	0.03	[-0.02, 0.10]
e) Sympathizing with the corporation			
Indirect	0.00	0.01	[-0.03, 0.02]
Direct	**0.23**	**0.04**	**[0.15, 0.30]**
Total	**0.23**	**0.04**	**[0.15, 0.30]**

Note. OPL = Online privacy literacy. Indirect effects were estimated with online privacy literacy at its mean value ($M = 5.54$) using the bootstrapping method. Significant relationships are highlighted in bold.

sympathizing with the corporation ($b^* = -0.01$, $p = .832$, 95% CI [−0.09, 0.07]), failing to support H2c and H2e. Moreover, contrary to H2d, we found that perceived surveillance had a negative relationship with downplaying dataveillance cost – the more one felt surveilled, the less likely that they would downplay or minimize the cost and harm of dataveillance, $b^* = -0.18$, $p < .001$, 95% CI [−0.24, −0.12]. Fig. 2 visualizes these relationships.

We also hypothesized that perceived surveillance should positively mediate the relationships between perceived accuracy and coping strategies (H3). As shown in Table 3, the indirect relationships of perceived accuracy via perceived surveillance on (a) intention to adjust ad settings and (b) privacy cynicism were significant and positive, supporting H3a and H3b. However, perceived surveillance did not mediate the relationships between perceived accuracy and (c) self-empowerment or (e) sympathizing. Contrary to H3d, we found a negative indirect relationship of perceived accuracy on (d) downplaying dataveillance cost through perceived surveillance.

In addition, perceived accuracy had a direct negative relationship with (a) intention to adjust ad settings, and direct positive relationships with (c) self-empowerment, (d) downplaying dataveillance cost, and (e) sympathizing with the corporation (see Table 3). Notably, for (a) intention to adjust ad settings and (d) downplaying dataveillance cost, the direct relationships were in the opposite directions to the indirect relationships between perceived accuracy and the two coping strategies, making the total relationships non-significant. Inferring from the total relationships, we found that perceived accuracy was overall positively related to (b) privacy cynicism, (c) self-empowerment, and (e) sympathizing with the corporation. People who perceived the algorithmic profiles to be more accurate were more likely to deem attempts of privacy protection futile. Meanwhile, they may also self-empower by reminding themselves of their existing attitude about Google and sympathize with Google by taking Google's perspective.

Regarding the moderating role of online privacy literacy on the relationships between perceived surveillance and the coping strategies (H4 and RQ1), opposite from H4b, online privacy literacy positively moderated the relationship between perceived surveillance and (b) privacy cynicism, $b^* = 0.08$, $p = .024$, 95% CI [0.01, 0.15]. Meanwhile, there was a negative relationship between online privacy literacy and privacy cynicism, $b^* = -0.16$, $p < .001$, 95% CI [−0.23, −0.09]. As shown in Fig. 3, for individuals with medium to high levels of online privacy literacy (Medium = 5.54, High = 6.51 on a 7-point scale), the more they experienced surveillance from Google, the more likely they would adopt privacy cynicism as a coping strategy. In contrast, this relationship did not exist for individuals with relatively low literacy as they report higher privacy cynicism regardless of their levels of

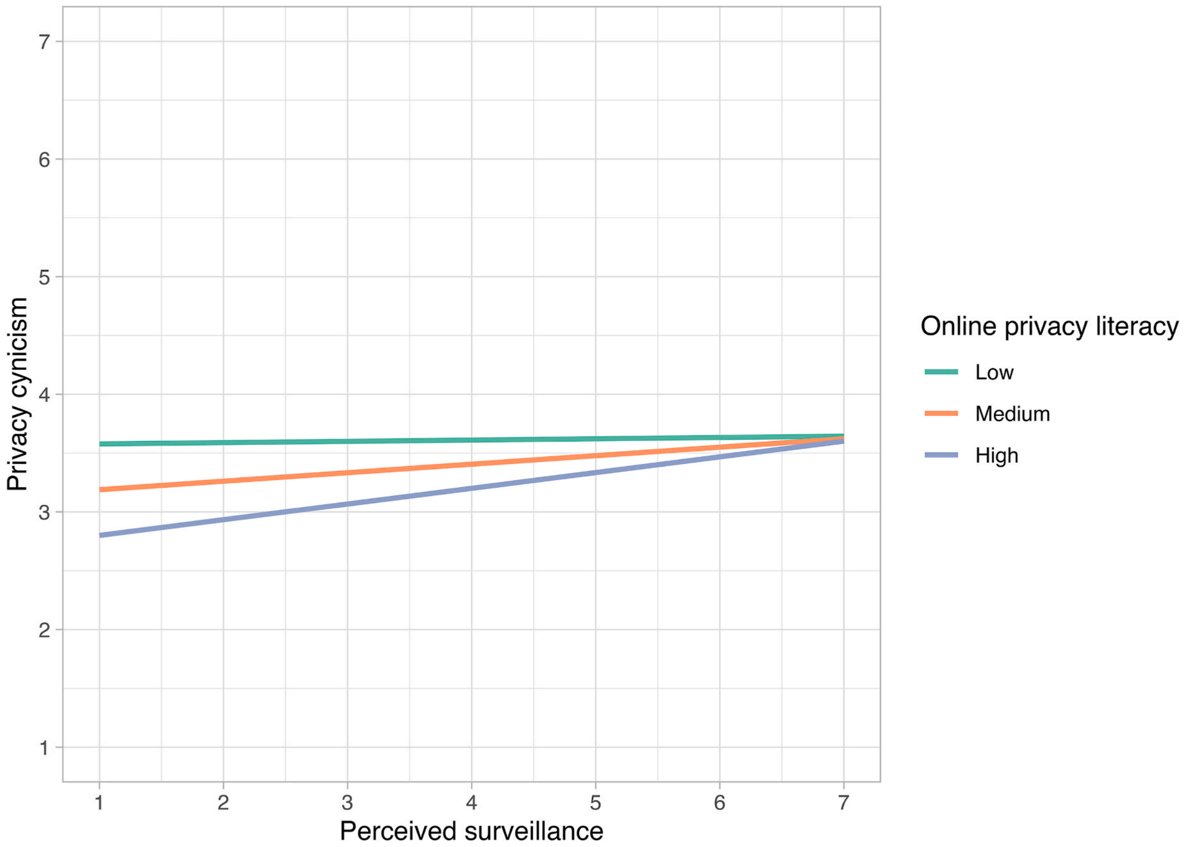

Fig. 3. Interaction between perceived surveillance and online privacy literacy on privacy cynicism.

perceived surveillance. For the other coping strategies, online privacy literacy did not moderate the relationships. Therefore, we did not find support for H4 overall. As for RQ1, online privacy literacy did not moderate the relationship between perceived surveillance and sympathizing with the corporation.

4.2. *Objective accuracy versus perceived accuracy*

To answer RQ2, we inspected the correlations between perceived accuracy and the two objective accuracy indicators: objective accuracy of sociodemographic inferences and objective accuracy of interest inferences. Perceived accuracy had a weak positive correlation with objective accuracy of sociodemographic inferences ($r = 0.15$, $p < .001$) and a moderate positive correlation with objective accuracy of interest inferences ($r = 0.46$, $p < .001$). The more Google correctly predicted one's interests and sociodemographic categories, the more likely the user perceived these inferences to be accurate. Interestingly, the two indicators of objective accuracy did not correlate with each other ($r = 0.01$, $p = .888$).

Regarding RQ3, we inspected the relationships between objective accuracy and perceived surveillance. As shown in Table 4, both indicators of objective accuracy had positive relationships with perceived surveillance ($b_{\text{sociodemo}}* = 0.11$; $b_{\text{interest}}* = 0.14$), but the relationships were weaker than the relationship between perceived accuracy and perceived surveillance ($b_{\text{perceived}}* = 0.31$).

As to the indirect relationships between objective accuracy and coping strategies through perceived surveillance inquired in RQ4, the objective accuracy of both types of inferences had similar but weaker indirect relationships with (a) intention to adjust ad setting ($b_{\text{perceived}}* = 0.10$, $b_{\text{sociodemo}}* = 0.03$, $b_{\text{interest}}* = 0.04$), (b) privacy cynicism ($b_{\text{perceived}}* = 0.03$, $b_{\text{sociodemo}}* = 0.01$, $b_{\text{interest}}* = 0.02$), and (d) downplaying dataveillance cost ($b_{\text{perceived}}* = -0.06$, $b_{\text{sociodemo}}* = -0.02$, $b_{\text{interest}}* = -0.02$). For (c) self-empowerment, while it was not indirectly related to perceived accuracy through perceived surveillance, it was indirectly related to both objective accuracy indicators ($b_{\text{sociodemo}}* = 0.02$, $b_{\text{interest}}* = 0.02$). Neither objective accuracy indicator had relationships with (e) sympathizing with the corporation, which is consistent with the finding from perceived accuracy.

5. Discussion

This study aimed to investigate the extent to which perceived accuracy of algorithmic profiling relates to individuals' perceived surveillance and coping strategies (i.e., intention to adjust ad settings, privacy cynicism, self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation). We highlight five key findings: (1) The more accurate one perceives their algorithmic profile to be, the more they feel surveilled; (2) perceived surveillance explains why people cope with perceived accuracy through privacy protection behavioral intention and privacy cynicism; (3) higher perceived accuracy is directly related to lower privacy protection behavioral intention, higher tendency of downplaying dataveillance cost, more self-empowerment, and more sympathizing with the corporation, while these relationships are not explained by perceived surveillance; (4) online privacy literacy does not always prevent people from experiencing privacy cynicism due to high perceived surveillance; (5) perceived accuracy holds greater importance than objective accuracy in shaping individuals' reactions.

The first key finding is that people who perceive their algorithmic profiles to be accurately reflecting themselves are also more likely to feel surveilled. This aligns with our argumentation using psychological ownership theory that accurate algorithmic inferences can be perceived as part of the individual's possession. Knowing that the company that produced the algorithmic profiles also has access to this information, individuals tend to experience higher perceived surveillance. This aligns

Table 4
Relationships between objective accuracy, perceived surveillance, online privacy literacy, and coping strategies.

Path	IV = Objective accuracy (sociodemographic inferences)			IV = Objective accuracy (interest inferences)		
	*b**	(Boot) *SE*	95% (Boot) CI	*b**	(Boot) *SE*	95% (Boot) CI
Perceived surveillance (PS)						
IV → PS	**0.11**	**0.04**	**[0.04, 0.18]**	**0.14**	**0.04**	**[0.07, 0.21]**
a) Intention to adjust ad settings (INT)						
PS → INT	**0.28**	**0.03**	**[0.22, 0.35]**	**0.28**	**0.03**	**[0.21, 0.34]**
IV → PS → INT (Indirect)	**0.03**	**0.01**	**[0.01, 0.06]**	**0.04**	**0.01**	**[0.02, 0.06]**
IV → INT (Direct)	−0.03	0.03	[-0.09, 0.04]	0.04	0.03	[-0.02, 0.10]
IV → INT (Total)	0.01	0.03	[-0.05, 0.07]	**0.08**	**0.03**	**[0.02, 0.15]**
PS × OPL → INT	0.01	0.03	[-0.05, 0.06]	0.02	0.03	[-0.03, 0.08]
b) Privacy cynicism (CYN)						
PS → CYN	**0.11**	**0.04**	**[0.03, 0.19]**	**0.12**	**0.04**	**[0.04, 0.20]**
IV → PS → CYN (Indirect)	**0.01**	**0.01**	**[0.00, 0.03]**	**0.02**	**0.01**	**[0.00, 0.03]**
IV → CYN (Direct)	0.03	0.04	[-0.05, 0.10]	−0.05	0.04	[-0.12, 0.03]
IV → CYN (Total)	0.05	0.04	[-0.02, 0.13]	−0.04	0.04	[-0.11, 0.03]
PS × OPL → CYN	**0.08**	**0.04**	**[0.01, 0.15]**	**0.08**	**0.04**	**[0.01, 0.15]**
c) Self-empowerment (SE)						
PS → SE	**0.18**	**0.04**	**[0.10, 0.25]**	**0.15**	**0.04**	**[0.08, 0.22]**
IV → PS → SE (Indirect)	**0.02**	**0.01**	**[0.01, 0.04]**	**0.02**	**0.01**	**[0.01, 0.04]**
IV → SE (Direct)	0.00	0.04	[-0.07, 0.07]	**0.20**	**0.04**	**[0.13, 0.27]**
IV → SE (Total)	0.02	0.04	[-0.05, 0.09]	**0.22**	**0.04**	**[0.15, 0.30]**
PS × OPL → SE	0.03	0.03	[-0.03, 0.10]	0.03	0.03	[-0.04, 0.09]
d) Downplaying dataveillance cost (DOWN)						
PS → DOWN	**−0.15**	**0.03**	**[-0.21, -0.09]**	**−0.15**	**0.03**	**[-0.21, -0.09]**
IV → PS → DOWN (Indirect)	**−0.02**	**0.01**	**[-0.03, 0.00]**	**−0.02**	**0.01**	**[-0.04, -0.01]**
IV → DOWN (Direct)	−0.01	0.03	[-0.06, 0.05]	0.06	0.03	[0.00, 0.12]
IV → DOWN (Total)	−0.02	0.03	[-0.08, 0.03]	0.04	0.03	[-0.02, 0.09]
PS × OPL → DOWN	0.04	0.03	[-0.01, 0.09]	0.04	0.03	[-0.01, 0.10]
e) Sympathizing with the corporation (SYM)						
PS → SYM	0.07	0.04	[-0.01, 0.14]	0.07	0.04	[-0.01, 0.14]
IV → PS → SYM (Indirect)	0.01	0.01	[0.00, 0.02]	0.01	0.01	[0.00, 0.02]
IV → SYM (Direct)	0.01	0.04	[-0.06, 0.08]	0.07	0.04	[-0.01, 0.14]
IV → SYM (Total)	0.02	0.04	[-0.06, 0.09]	**0.08**	**0.04**	**[0.01, 0.15]**
PS × OPL → SYM	0.04	0.04	[-0.03, 0.11]	0.02	0.03	[-0.05, 0.09]

Note. OPL = Online privacy literacy. Indirect effects were estimated with online privacy literacy at its mean value (M = 5.54) using the bootstrapping method. Significant relationships are highlighted in bold.

with previous works on algorithmic profiling, where users reported uncomfortableness after seeing their algorithmic profiles (Büchi et al., 2023). Given that one of the primary uses of algorithmic profiles is for ad personalization, future research should investigate whether highly personalized advertisements based on accurate algorithmic profiles would also be related to increased perceived surveillance.

Second, as individuals experience more perceived surveillance, they tend to cope by increasing the intention to adjust ad settings and resorting to privacy cynicism. This suggests that perceived surveillance indeed triggers psychological reactance (Brehm & Brehm, 1981). However, people may only cope with it by either being more inclined to engage in privacy protection behavior, or the contrary—resorting to privacy cynicism and deeming privacy protection behavior futile. Our findings suggest that the most commonly used strategies by individuals to cope with perceived surveillance might be privacy protection behavior and privacy cynicism. Both coping strategies have been examined relatively extensively in the literature (e.g., Baruh et al., 2017; Boerman et al., 2021; Lutz et al., 2020), which indicates their prevalence as coping responses. Contrary to our expectation, we found that the more people feel surveilled, the less likely they would adopt the downplaying coping strategy. This suggests that in the context of algorithmic profiling, feeling surveilled would remind people of the negative aspects of dataveillance so that people are less likely to diminish the cost of dataveillance. Future research could examine the contextual factors influencing the adoption of different coping strategies, identifying the specific situations in which individuals are likely to adopt each strategy.

Third, while perceived surveillance can explain part of the mechanism regarding why people cope with algorithmic profiling, it is not the sole factor mediating this relationship. Besides the relationships explained by perceived surveillance, perceived accuracy also has direct relationships with all coping strategies except privacy cynicism. This suggests that in parallel with perceived surveillance, there might be other mediators that play the opposite role and suppress psychological reactance. One potential alternative mechanism could be that when the algorithmic profile is perceived to be accurate, people might develop more trust in the platform's competence in offering high-quality personalized experiences for them (S. Chen & Dhillon, 2003; X. Chen, Sun, & Liu, 2022; Liu & Tao, 2022), thus are less likely to limit data access through privacy protection behavior, and more likely to adopt cognitive coping strategies that enable them to continue enjoying the benefits of algorithmic profiling. Another potential mediator could be surprise: negative surprise can manifest as the result of seeing either too accurate or too inaccurate algorithmic profiles (Büchi et al., 2023; Hautea et al., 2020). In both cases, users may feel the need to deal with the negative affect. Future research should explore these potential mediators to better understand the complex relationship between perceived accuracy and coping strategies.

Fourth, our results revealed a conditional role of online privacy literacy regarding the relationship between perceived surveillance and privacy cynicism. Contrary to our expectation, there is a stronger relationship between perceived surveillance and privacy cynicism among people who evaluate themselves with medium or high online privacy literacy, while people who report lower literacy experience relatively high privacy cynicism regardless of how much they feel surveilled. This may indicate that privacy cynicism is a constant coping strategy rather than a reactive response to perceived surveillance for people with lower literacy. Previous research has shown that privacy or internet literacy equips oneself with the agency against privacy cynicism (Lutz et al., 2020; Masur, 2020). Our finding adds more nuance to this argument by showing that even people with relatively high literacy may still resort to privacy cynicism when they feel surveilled, which suggests that knowing how to protect one's privacy online does not necessarily mean one possesses higher agency or self-efficacy. Additionally, the non-significance of the interaction relationships with other coping strategies could be attributed to a ceiling effect: on average, our participants scored 5.54 out of 7 on the online privacy literacy scale, indicating a relatively high level of self-confidence in their privacy literacy. This is not surprising given that they were recruited via an online panel and were able to follow the multi-step instructions to access their algorithmic profiles. Therefore, we recommend that future research investigating the role of online privacy literacy make extra efforts to ensure a diverse sample of individuals across different levels of online privacy literacy.

Last, while there is a weak association between perceived and objective accuracy, perceived accuracy seems to be a stronger predictor of perceived surveillance and coping strategies compared to objective accuracy. This finding corroborates with previous literature that differentiates perceived and actual personalization as well as interactivity (Li, 2016; Voorveld et al., 2011), suggesting that individuals' subjective evaluation of a particular quality in a technical system shapes subsequent user responses more than the objective quality of the system. The perceived accuracy is only to some extent based on the objective accuracy of the algorithm, meaning other factors may play a role when people evaluate the accuracy, for example, their preexisting beliefs that an algorithm is always precise (i.e., machine heuristics; Sundar & Kim, 2019, pp. 1–9). Users may have certain expectations on how well an algorithm should know them, and it could be that a few unexpected inferences (either too accurate or too inaccurate) dominantly affect perceived accuracy. Future research is needed to investigate the factors contributing to the discrepancies between perceived accuracy and objective accuracy. We also found a stronger correlation between perceived accuracy and objective accuracy based on interest inferences than objective accuracy based on sociodemographic inferences, which could indicate that perceived accuracy is attributed more to the prediction precision of interests than sociodemographic categories. Interestingly, the two indicators of objective accuracy do not correlate, which may suggest that Google employs different algorithms for these two types of inferences that make their objective performances differ. Future research should consider the differences among profiling mechanisms when investigating their influence on individual responses.

5.1. *Theoretical implications*

This study makes its first theoretical contribution by demonstrating that perceived accuracy of algorithmic profiling is a key driver for perceived surveillance and multiple types of individual coping. Extending from previous studies that captured individuals' initial reactions to their algorithmic profiles (Büchi et al., 2023; Hautea et al., 2020), this study looks further into how algorithmic profiles can have profound implications on the psychological processes of individuals.

Second, this finding extends the DEAL framework concerning the antecedents of perceived surveillance (Strycharz & Segijn, 2022). While the DEAL framework proposes that any instance of a surveillance episode may induce perceived surveillance, it is not specified whether the features of a surveillance episode could influence the extent to which people feel surveilled. This study demonstrates that depending on the features of a surveillance episode, such as perceived accuracy, individuals can experience varying degrees of perceived surveillance. Future research could explore additional features in individuals' dataveillance experiences that might influence the intensity of perceived surveillance.

Third, whereas most existing literature in the context of dataveillance examined each coping strategy independently, this study builds upon the latest typology of how people cope with dataveillance (Zhang et al., 2024) and quantitatively establishes the relationships between perceived surveillance and five distinct types of coping strategies. The findings contribute to our understanding of how and why individuals cope in different ways. Under high psychological reactance (i.e., when perceived surveillance is triggered), individuals tend to resort to privacy protection behavior and privacy cynicism, whereas self-empowerment, downplaying, and sympathizing are driven by being exposed to the surveillance episode directly. It is also noteworthy that, overall, people do *not* cope with perceived accuracy by engaging in privacy protection behavior. This may be because cognitive coping strategies, such as privacy cynicism, effectively resolve cognitive dissonance and emotional tension caused by perceived surveillance (Hoffmann et al., 2016; Lutz et al., 2020; Ranzini, Lutz, & Hoffmann, 2023). Applying the protection motivation theory (Rogers, 1975), a widely-used theory to examine antecedents of privacy protection behavior, the reason why individuals tend to cope through privacy cynicism rather than privacy protection could also be that individuals perceive low self-efficacy and/or response efficacy (Boerman et al., 2021). Future research could validate this finding and further investigate the underlying mechanisms.

Fourth, this study consolidates the conceptual distinction between perceived and objective accuracy and offers evidence that perceived accuracy holds greater importance than objective accuracy in shaping individuals' reactions. This resonates with existing calls for a paradigm shift in algorithmic system development to put greater focus on the psychological mechanisms underlying user interactions with algorithmic systems (e.g., Grill & Andalibi, 2022). This finding underscores the need for researchers, platform developers, and policymakers to prioritize not only the objective accuracy of algorithmic systems but also users' subjective perceptions of accuracy in designing a trustworthy system and developing effective interventions to address concerns related to privacy and dataveillance.

5.2. *Practical implications*

The findings of this study offer significant societal implications by shedding light on how individuals perceive and react to algorithmic profiling and dataveillance in their daily lives. From a consumer empowerment perspective, privacy dashboards such as the Google My Ad Center were designed to provide users with more information and control over their personal data as an attempt to signal transparency (Büchi et al., 2023). However, when users are confronted with the extensive profiling categories, it becomes evident that dataveillance takes place in their everyday lives, potentially provoking feelings of being surveilled and vulnerability (Büchi et al., 2022). Furthermore, when algorithmic profiles are perceived as inaccurate, users may experience lower perceived surveillance, leading to a false sense of security that undermines awareness of privacy risks.

In addition, our study revealed that only a small proportion of participants had previously accessed their algorithmic profile. By exposing individuals to their algorithmic profiles, the study raised awareness about the existence of such profiles for many participants and suggested a potential avenue for intervention designs. It has been a persistent challenge to develop interventions that effectively promote privacy protection behavior, as multiple approaches, including increasing knowledge and increasing awareness of the privacy threat, have been proven to be ineffective (Boerman, Strycharz, & Smit, 2024; Strycharz, Noort, Smit, & Helberger, 2019, 2021; Stubenvoll & Binder, 2024). This procedure may serve as an intervention strategy to encourage privacy protection behavior, as we found that people show increased intention to change their ad settings due to heightened perceived surveillance. However, it should be noted with caution that this is also accompanied by increased feelings of privacy cynicism, which may hinder privacy protection behavior (Choi, Park, & Jung, 2018). Future research could explore how to leverage perceived surveillance to motivate people to take action while also not inducing privacy cynicism, for example, by accompanying the surveillance episode with training that increases one's self-efficacy and response efficacy (see Boerman et al., 2024). As such, this study contributes to the ongoing effort to develop effective consumer empowerment interventions by proposing an additional potential intervention strategy.

5.3. Limitations

We acknowledge several limitations in this study. First, our study examined algorithmic profiles from Google, which primarily contain sociodemographic and interest inferences, whereas other platforms might use different types of profiles, potentially influencing the observed relationships. Second, the cross-sectional survey design of the study limits our ability to establish causal relationships, restricting cause-and-effect interpretations. Third, our sample was drawn exclusively from the UK population, which may limit the generalizability of the findings to other cultural contexts or societies. Fourth, participants in our study exhibited relatively high levels of online privacy literacy, which may not represent the average population. Lastly, the reliance on self-reported measures for constructs related to individual perceptions could introduce the potential for biases, such as social desirability bias.

6. Conclusions

This study explores the relationships between perceived accuracy of algorithmic profiling, individuals' perceived surveillance, and their subsequent coping mechanisms. The findings reveal that the more individuals perceive their algorithmic profiles as accurate reflections of themselves, the more they tend to feel surveilled. This heightened feeling of surveillance is associated with a range of coping responses, including privacy cynicism and intentions to adopt privacy protection behavior. The study also found that individuals with high online privacy literacy are less likely to experience privacy cynicism when their perceived surveillance is low. By elucidating the connections between algorithmic profiling and individual responses, the study deepens our understanding of how individuals react to algorithmic profiling, a dataveillance practice that has been woven into their everyday digital lives.

CRediT authorship contribution statement

Dong Zhang: Writing – review & editing, Writing – original draft, Visualization, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Joanna Strycharz:** Writing – review & editing, Supervision, Resources, Methodology, Conceptualization. **Sophie C. Boerman:** Writing – review & editing, Supervision, Methodology, Conceptualization. **Theo Araujo:** Writing – review & editing, Supervision, Methodology, Conceptualization. **Hilde Voorveld:** Writing – review & editing, Supervision, Methodology, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by Amsterdam School of Communication Research, University of Amsterdam.

Data availability

Anonymized data and code for analysis are available at: https://osf.io/hbt4d/

References

Bansal, G., Zahedi, F., Mariam, & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Barbosa, N. M., Wang, G., Ur, B., & Wang, Y. (2021). Who am I? A design probe exploring real-time transparency about online and offline user profiling underlying targeted ads. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 5*(3), 1–88:32. https://doi.org/10.1145/3478122, 88.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bashir, M. A., Farooq, U., Shahid, M., Zaffar, M. F., & Wilson, C. (2019). Quantity vs. quality: Evaluating user interest profiles using ad preference managers. *Proceedings 2019 Network and distributed system security symposium. Network and distributed system security symposium*. https://doi.org/10.14722/ndss.2019.23392. San Diego, CA.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953–977. https://doi.org/10.1177/0093650218800915

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

Brehm, S. S., & Brehm, J. W. (1981). *Psychological reactance: A theory of freedom and control*. Academic Press.

Briñol, P., Rucker, D. D., Tormala, Z. L., & Petty, R. E. (2004). Individual differences in resistance to persuasion: The role of beliefs and meta-beliefs. In E. S. Knowles, & J. A. Linn (Eds.), *Resistance and persuasion* (pp. 83–104). Lawrence Erlbaum Associates.

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society, 9*(1), Article 20539517211065368. https://doi.org/10.1177/20539517211065368

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., & Velidi, S. (2023). Making sense of algorithmic profiling: User perceptions on Facebook. *Information, Communication & Society, 26*(4), 809–825. https://doi.org/10.1080/1369118X.2021.1989011

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review, 36*, Article 105367. https://doi.org/10.1016/j.clsr.2019.105367

Chen, S. C., & Dhillon, G. S. (2003). Interpreting dimensions of consumer trust in E-commerce. *Information Technology and Management, 4*(2), 303–318. https://doi.org/10.1023/A:1022962631249

Chen, L., & Pu, P. (2009). Interaction design guidelines on critiquing-based recommender systems. *User Modeling and User-Adapted Interaction, 19*(3), 167–206. https://doi.org/10.1007/s11257-008-9057-x

Chen, X., Sun, J., & Liu, H. (2022). Balancing web personalization and consumer privacy concerns: Mechanisms of consumer trust and reactance. *Journal of Consumer Behaviour, 21*(3), 572–582. https://doi.org/10.1002/cb.1947

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Cichy, P., Salge, T.-O., & Kohli, R. (2014). Extending the privacy calculus: The role of psychological ownership. *ICIS 2014 Proceedings, 30*, 1–19. https://aisel.aisnet.org/icis2014/proceedings/ISSecurity/30.

Davis, M. H. (1980). A multidimensional approach to individual differences in empathy. *JSAS Catalog of Selected Documents in Psychology, 10*, 85.

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

Eke, C. I., Norman, A. A., Shuib, L., & Nweke, H. F. (2019). A survey of user profiling: State-of-the-art, challenges, and solutions. *IEEE Access, 7*, 144907–144924. https://doi.org/10.1109/ACCESS.2019.2944243. IEEE Access.

Eslami, M., Krishna Kumaran, S. R., Sandvig, C., & Karahalios, K. (2018). Communicating algorithmic process in online behavioral advertising. *Proceedings of the 2018 CHI conference on human factors in computing systems*. https://doi.org/10.1145/3173574.3174006

Fairclough, S. H., Karran, A. J., & Gilleade, K. (2015). Classification accuracy from the perspective of the user: Real-time interaction with physiological computing. *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. https://doi.org/10.1145/2702123.2702454

Farman, L., Comello, M. L., Nori, & Edwards, J. R. (2020). Are consumers put off by retargeted ads on social media? Evidence for perceptions of marketing surveillance and decreased ad effectiveness. *Journal of Broadcasting & Electronic Media, 64*(2), 298–319. https://doi.org/10.1080/08838151.2020.1767292

Fransen, M. L., Smit, E. G., & Verlegh, P. W. J. (2015). Strategies and motives for resistance to persuasion: An integrative framework. *Frontiers in Psychology, 6*. https://www.frontiersin.org/articles/10.3389/fpsyg.2015.01201.

Frener, R., Dombrowski, J., & Trepte, S. (2023). Development and validation of the need for privacy scale (NFP-S). *Communication Methods and Measures, 0*(0), 1–24. https://doi.org/10.1080/19312458.2023.2246014

Google. (n.d.). *Getting started with My Ad Center*. My Ad Center Help. Retrieved November 7, 2023, from https://support.google.com/My-Ad-Center-Help/answer/12155154?hl=en.

Grill, G., & Andalibi, N. (2022). Attitudes and folk theories of data subjects on transparency and accuracy in emotion recognition. *Proceedings of the ACM on Human-Computer Interaction, 6*(78), 1–78:35. https://doi.org/10.1145/3512925. CSCW1.

Hautea, S., Munasinghe, A., & Rader, E. (2020). "That's not me": Surprising algorithmic inferences. *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–7. https://doi.org/10.1145/3334480.3382816

Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (3rd ed.). The Guilford Press.

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

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

Kappeler, K., Festic, N., & Latzer, M. (2023). Dataveillance imaginaries and their role in chilling effects online. *International Journal of Human-Computer Studies, 103120*. https://doi.org/10.1016/j.ijhcs.2023.103120

Kim, E., & Huh, J. (2023). Intentional viewing of skippable ads on YouTube: An exploratory study. In A. Vignolles, & M. K. J. Waiguny (Eds.), *Advances in advertising research (vol. XII): Communicating, designing and consuming authenticity and narrative* (pp. 81–96). Springer Fachmedien. https://doi.org/10.1007/978-3-658-40429-1_6.

Knowles, E. S., & Linn, J. A. (2004). *Resistance and persuasion*. Lawrence Erlbaum Associates.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction, 2*(CSCW), 102:1–102:31. https://doi.org/10.1145/3274371

Li, C. (2016). When does web-based personalization really work? The distinction between actual personalization and perceived personalization. *Computers in Human Behavior, 54*, 25–33. https://doi.org/10.1016/j.chb.2015.07.049

Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior, 127*, Article 107026. https://doi.org/10.1016/j.chb.2021.107026

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society, 22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society, 6*(2), Article 2053951719895805. https://doi.org/10.1177/2053951719895805

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

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication, 8*(2). https://doi.org/10.17645/mac.v8i2.2855. Article 2.

Masur, P. K., Hagendorff, T., & Trepte, S. (2023). Challenges in studying social media privacy literacy. In *The routledge handbook of privacy and social media*. Routledge.

Meier, Y., Schäwel, J., Kyewski, E., & Krämer, N. C. (2020). Applying protection motivation theory to predict Facebook users' withdrawal and disclosure intentions. *International Conference on Social Media and Society*, 21–29. https://doi.org/10.1145/3400806.3400810

Meta. (n.d.). Ad preferences. Facebook Help Center. Retrieved November 7, 2023, from https://www.facebook.com/help/109378269482053.

Meyvis, T., & van Osselaer, S. M. J. (2018). Increasing the power of your study by increasing the effect size. *Journal of Consumer Research, 44*(5), 1157–1173. https://doi.org/10.1093/jcr/ucx110

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. In *The black box society*. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology, 7*(1), 84–107. https://doi.org/10.1037/1089-2680.7.1.84

Piotrowski, J., Vries, D. A. de, & Vreese, C. de (2021). Digital competence across the lifespan. https://osf.io/d5c7n/.

Pollay, R. W., & Mittal, B. (1993). Here's the beef: Factors, determinants, and segments in consumer criticism of advertising. *Journal of Marketing, 57*(3), 99–114. https://doi.org/10.1177/002224299305700307

Pu, P., Chen, L., & Hu, R. (2012). Evaluating recommender systems from the user's perspective: Survey of the state of the art. *User Modeling and User-Adapted Interaction, 22*(4), 317–355. https://doi.org/10.1007/s11257-011-9115-7

Rader, E., Hautea, S., & Munasinghe, A. (2020). "I have a narrow thought process": Constraints on explanations connecting inferences and self-perceptions. *Proceedings of the sixteenth USENIX conference on useable privacy and security*.

Ranzini, G., Lutz, C., & Hoffmann, C. P. (2023). Privacy cynicism: Resignation in the face of agency constraints. In S. Trepte, & P. Masur (Eds.), *The routledge handbook of privacy and social media* (1st ed., pp. 134–143). Routledge. https://doi.org/10.4324/9781003244677-15.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Segijn, C. M., Kim, E., Lee, G., Gansen, C., & Boerman, S. C. (2023). The intended and unintended effects of synced advertising: When persuasion knowledge could help or backfire. *International Journal of Research in Marketing*. https://doi.org/10.1016/j.ijresmar.2023.07.001

Segijn, C. M., Kim, E., Sifaoui, A., & Boerman, S. C. (2023). When you realize that big brother is watching: How informing consumers affects synced advertising effectiveness. *Journal of Marketing Communications, 29*(4), 317–338. https://doi.org/10.1080/13527266.2021.2020149

Segijn, C. M., Opree, S. J., & Ooijen, I. van (2022). The validation of the perceived surveillance scale. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16*(3). https://doi.org/10.5817/CP2022-3-9. Article 9.

Segijn, C. M., & van Ooijen, I. (2020). Perceptions of techniques used to personalize messages across media in real time. *Cyberpsychology, Behavior, and Social Networking, 23*(5), 329–337. https://doi.org/10.1089/cyber.2019.0682

Sifaoui, A. (2021). We know what you see, so here's an ad. Online behavioral advertising and surveillance on social media in an era of privacy erosion [University of Minnesota] http://conservancy.umn.edu/handle/11299/224475.

Sifaoui, A., Lee, G., & Segijn, C. M. (2023). Brand match vs. Mismatch and its impact on avoidance through perceived surveillance in the context of synced advertising. In A. Vignolles, & M. K. J. Waiguny (Eds.), *Advances in advertising research (vol. XII): Communicating, designing and consuming authenticity and narrative* (pp. 137–147). Springer Fachmedien. https://doi.org/10.1007/978-3-658-40429-1_10.

Similarweb. (n.d.). Google.com traffic analytics, *ranking stats & tech stack*. Similarweb. Retrieved November 2, 2023, from https://www.similarweb.com/website/google.com/.

Strycharz, J., Kim, E., & Segijn, C. M. (2022). Why people would (not) change their media use in response to perceived corporate surveillance. *Telematics and Informatics, 71*, Article 101838. https://doi.org/10.1016/j.tele.2022.101838

Strycharz, J., Noort, G. van, Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13*(2). https://doi.org/10.5817/CP2019-2-1. Article 2.

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

Strycharz, J., Smit, E., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior, 120*, Article 106750. https://doi.org/10.1016/j.chb.2021.106750

Stubenvoll, M., & Binder, A. (2024). Is knowledge power? Testing whether knowledge affects chilling effects and privacy-protective behaviors using browser histories. *Computers in Human Behavior, 150*, Article 107949. https://doi.org/10.1016/j.chb.2023.107949

Sundar, S. S., & Kim, J. (2019). Machine heuristic: When we trust computers more than humans with our personal information. *Proceedings of the 2019 CHI conference on human factors in computing systems*. https://doi.org/10.1145/3290605.3300768

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. *Proceedings of the eighth symposium on useable privacy and security*. https://doi.org/10.1145/2335356.2335362

van Dijk, E., & van Knippenberg, D. (2005). Wanna trade? Product knowledge and the perceived differences between the gains and losses of trade. *European Journal of Social Psychology, 35*(1), 23–34. https://doi.org/10.1002/ejsp.230

Voorveld, H. A. M., Meppelink, C. S., & Boerman, S. C. (2023). Consumers' persuasion knowledge of algorithms in social media advertising: Identifying consumer groups based on awareness, appropriateness, and coping ability. *International Journal of Advertising, 0*(0), 1–27. https://doi.org/10.1080/02650487.2023.2264045

Voorveld, H. A. M., Neijens, P. C., & Smit, E. G. (2011). The relation between actual and perceived interactivity. *Journal of Advertising, 40*(2), 77–92. https://doi.org/10.2753/JOA0091-3367400206

Zhang, D., Boerman, S. C., Hendriks, H., Araujo, T., & Voorveld, H. (2023). A peak into individuals' perceptions of surveillance. In A. Vignolles, & M. K. J. Waiguny (Eds.), *Advances in advertising research (vol. XII): Communicating, designing and consuming authenticity and narrative* (pp. 163–178). Springer Fachmedien. https://doi.org/10.1007/978-3-658-40429-1_12.

Zhang, D., Boerman, S. C., Hendriks, H., van der Goot, M. J., Araujo, T., & Voorveld, H. (2024). "They know everything": Folk theories, thoughts, and feelings about dataveillance in media technologies. *International Journal of Communication, 18*, 2710–2730.