

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, and Hilde Voorveld^a

^aAmsterdam School of Communication Research, University of Amsterdam, Amsterdam, The Netherlands; ^bStrategic Communication, Wageningen University & Research, Wageningen, The Netherlands

Nieuwe Achtergracht 166, 1018 WV Amsterdam, The Netherlands; email:
d.zhang@uva.nl

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

Enabled by the ubiquitous dataveillance practices, corporations construct accurate algorithmic profiles about their users for personalized advertising. This study employs 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 two positive relationships mediated by perceived surveillance: as individuals perceive their algorithmic profiles with greater accuracy, they report heightened feelings of surveillance, which is also associated with increased intentions of adjusting ad settings and privacy cynicism. Meanwhile, perceived surveillance is negatively associated with downplaying dataveillance costs. Furthermore, individuals who perceive their algorithmic profiles to be more accurate also tend to cope by empowering themselves and sympathizing with the corporation, while these relationships are not explained by perceived surveillance.

Keywords: algorithmic profiling, dataveillance, accuracy, perceived surveillance, coping, privacy cynicism

Introduction

Nowadays, individuals are constantly subjected to the automated, continuous, and unspecific collection, storage, and processing of their digital traces (i.e., dataveillance; Büchi, Festic, and Latzer 2022; Strycharz and Segijn 2022). Leveraging these data, corporations can create accurate algorithmic profiles for personalized advertising (Voorveld, Meppelink, and Boerman 2023). These algorithmic profiles often include inferences regarding one's interests and demographic characteristics. When users encounter highly accurate inferences, they quickly realize that their personal data have been used to curate these profiles (Büchi et al. 2023; Hautea, Munasinghe, and Rader 2020; Rader, Hautea, and Munasinghe 2020). A directly observable instance of data collection like this can induce perceived surveillance, and subsequently prompt surveillance responses (Strycharz and Segijn 2022). These responses, including privacy

protection behavior and a number of cognitive strategies such as privacy cynicism (Zhang et al. in press), are employed by individuals to deal with and rationalize the uneasiness induced by perceived surveillance (i.e., coping). As individuals become increasingly aware of algorithmic profiling practices (Voorveld, Meppelink, and Boerman 2023), we aim to investigate the relationship between the perceived accuracy of algorithmic profiling, perceived surveillance, and subsequent coping responses in the current study.

Theoretical framework

We postulate that the perceived accuracy of algorithmic profiling is positively linked to perceived surveillance. This relationship can be explained by the theory of psychological ownership (Pierce, Kostova, and Dirks 2003). Psychological ownership emerges when individuals feel familiar, associated with, or have intimate knowledge of the target (van Dijk and van Knippenberg 2005). The more accurate an inference is, the more intimate and knowledgeable one might feel towards this information, which intensifies the sense of ownership. In such cases, realizing that a company also knows about this information may heighten the feeling of being surveilled (Segijn, Kim, Lee, et al. 2023; Segijn, Kim, Sifaoui, et al. 2023). This leads to our first hypothesis:

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

Perceived surveillance can threaten an individual's sense of control and freedom of determining what the company can or cannot know about themselves, which motivates them to resist this perceived influence (Brehm and Brehm 1981). This psychological reactance can be mitigated in different ways. When one sees the algorithmic profile and wants to mitigate the extent to which they are being surveilled, the most probable coping behavior is to adjust the ad settings on the platform as a form

of privacy-protection behavior (Boerman, Strycharz, and Smit 2023). Moreover, existing studies have identified several cognitive strategies individuals employ to cope with the discomfort of perceived surveillance: privacy cynicism, self-empowerment, downplaying surveillance cost, and sympathizing (Zhang et al. in press). Privacy cynicism is an attitude of uncertainty, powerlessness, and mistrust towards the handling of personal data by digital platforms while perceiving privacy protection as being futile (Hoffmann, Lutz, and Ranzini 2016; Lutz, Hoffmann, and Ranzini 2020). Self-empowerment, contrarily, is to reaffirm oneself with arguments that support their current attitudes and behavior, which has been referred to as *attitude bolstering* in the persuasion literature (Jacks and Cameron 2003). Downplaying surveillance cost means one diminishes the threat of being surveilled with arguments such as “nothing to hide, nothing to lose” (Marwick and Hargittai 2019). Lastly, people may also sympathize with the corporation because they understand why companies need to make inferences (e.g., to generate revenue to provide free services) (Zhang et al. in press). All five surveillance responses should be positively related to perceived surveillance as they are different ways to minimize psychological reactance. Thus, we hypothesize that:

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

Furthermore, we hypothesize that perceived surveillance plays a mediating role in this process:

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 data surveillance cost; and (e) sympathizing with the corporation.

We also consider online privacy literacy as an individual differences that might influence the relationship between perceived surveillance and coping. It is defined as a combination of factual privacy knowledge, privacy-related reflection abilities, privacy and data protection skills, and critical privacy literacy (Masur, Hagendorff, and Trepte 2023). Users with higher online privacy literacy are not only more capable of deploying privacy-protection behaviors (Bartsch and Dienlin 2016; Baruh, Secinti, and Cemalcilar 2017; Park 2013), but also possess more agency to pursue their own goals (Masur 2020). Following this argument, we postulate that having high literacy empowers users when facing the threat of dataveillance, so that they cope with perceived surveillance by approaching the issue, either through increasing their intention of adjusting ad settings or self-empowerment. Contrarily, for users with lower levels of literacy, due to their lack of agency, perceived surveillance is more likely to induce passive ways of coping such as privacy cynicism and downplaying dataveillance cost. We hypothesize:

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.

Additionally, we explore whether and how online privacy literacy moderates the relationship between perceived surveillance and sympathizing with the corporation due to the currently limited literature on this matter:

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

Perceived accuracy and objective accuracy

Individuals' subjective evaluation of algorithmic profiles may be related to the objective accuracy of the algorithmic profiles – the extent to which the algorithmic

inferences correctly reflect individuals' actual traits and interests. This parallel between objective and perceived accuracy echoes similar relationships seen in actual versus perceived personalization (Li 2016), and objective versus subjective persuasion knowledge (Carlson et al. 2009). While perceived accuracy has a more direct influence on user trust and behavioral intentions (L. Chen and Pu 2009), evidence remains inconclusive regarding its relationship with objective accuracy (Pu, Chen, and Hu 2012). Users may perceive inferences based on their actual online behaviors to be inaccurate, or they might find justification for objectively inaccurate results to be accurate (Barbosa et al. 2021; Eslami et al. 2018). We thus ask:

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

Furthermore, we explore whether there is any relationship between objective accuracy, perceived surveillance, and coping responses:

RQ3. How does objective accuracy of algorithmic profiling relate to perceived surveillance and (a) intention to adjust ad settings; (b) privacy cynicism; (c) self-empowerment; (d) downplaying data surveillance cost; and (e) sympathizing with the corporation?

The conceptual model is visualized in Figure 1.

[Figure 1 near here]

Methods

Design and sample

We conducted a cross-sectional survey in which we asked participants to inspect their actual algorithmic profiles on Google. The survey utilized a quota sample mirroring the adult population in the United Kingdom ($N = 685$) and was distributed via Prolific.

Participants were 45.5 years old on average ($SD = 15.2$). 50.8% identified as female. Most participants completed undergraduate education (45.3%) or postgraduate education (21.9%). The majority (60.7%) had never heard of or visited Google My Ad Center (the webpage that contains the algorithmic profiles) prior to their participation.

Procedure

Upon giving informed consent, eligible participants were instructed to inspect the inferred interests and sociodemographic categories in their Google My Ad Center. 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 content of both pages they visited in their Google My Ad Center and answered questions for computing the objective accuracy. Lastly, we measured participants' online privacy literacy, potential covariates, and demographic information.

Measures

We measured perceived accuracy and objective accuracy of algorithmic profiling, perceived surveillance, online privacy literacy, and five coping strategies: intention to adjust ad settings, privacy cynicism, downplaying dataveillance cost, and sympathizing with the corporation. We also included four potential covariates: prior attitude towards personalized advertising on Google, need for privacy, and internet privacy concerns. Details can be found in Table 1.

[Table 1 near here]

Results

Perceived accuracy, perceived surveillance, and coping

We tested H1-H4, RQ1, and RQ3 with model 14 of the PROCESS macro using 5,000 bootstrap samples (Hayes, 2022). In line with H1, perceived accuracy was positively related to perceived surveillance, $b^* = 0.31, p < .001, 95\% \text{ CI } [0.24, 0.37]$.

As for H2, perceived surveillance had positive relationships with intention to adjust ad settings ($b^* = 0.32, p < .001, 95\% \text{ CI } [0.25, 0.39]$) and privacy cynicism ($b^* = 0.09, p = .024, 95\% \text{ CI } [0.01, 0.18]$), supporting H2a and H2b. Perceived surveillance was not related to self-empowerment ($b^* = 0.03, p = .479, 95\% \text{ CI } [-0.05, 0.10]$) and sympathizing with the corporation ($b^* = -0.01, p = .832, 95\% \text{ CI } [-0.09, 0.07]$), failing to support H2c and H2e. Moreover, contrary to H2d, we found that perceived surveillance had a negative relationship with downplaying dataveillance cost, $b^* = -0.18, p < .001, 95\% \text{ CI } [-0.24, -0.12]$. Figure 2 visualizes these relationships.

[Figure 2 near here]

Regarding H3, as shown in Table 2, 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 as well as (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 2). Inferring from the total relationships, perceived accuracy

was overall positively related to (b) privacy cynicism, (c) self-empowerment, and (e) sympathizing with the corporation.

[Table 2 near here]

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]. As shown in Figure 3, for people with medium to high levels of online privacy literacy, the more they experienced surveillance from Google, the more likely they would cope through privacy cynicism, whereas this relationship did not exist for people with relatively low literacy. For the other coping strategies, online privacy literacy did not moderate the relationships. Therefore, we did not find support for H4 overall and RQ1.

[Figure 3 near here]

Objective accuracy vs. perceived accuracy

Answering RQ2, perceived accuracy had a weak positive correlation with objective accuracy for sociodemographic inferences ($r = .15$, $p < .001$), and a moderate positive correlation with objective accuracy for interest inferences ($r = .46$, $p < .001$).

Regarding RQ3, as shown in Table 3, both indicators of objective accuracy had positive relationships with perceived surveillance, but the relationships were weaker than the relationship between perceived accuracy and perceived surveillance. Objective accuracy for both types of inferences had similar but weaker indirect relationships with (a) intention to adjust ad setting, (b) privacy cynicism, and (d) downplaying dataveillance cost compared to perceived accuracy. 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. Neither objective accuracy

indicator had relationships with (e) sympathizing with the corporation, which is consistent with the finding from perceived accuracy.

[Table 3 near here]

Discussion

This study aims 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.

First, people who perceive their algorithmic profiles as an accurate reflection of themselves are more likely to feel surveilled. This aligns with previous works on algorithmic profiling, where users reported uncomfortableness after seeing their algorithmic profiles (Büchi et al. 2023). The finding also echoes studies in personalized advertising, where it has been found that more personalized persuasion attempts trigger perceived surveillance (Sifaoui 2021).

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 and Brehm 1981), but the most commonly used strategies by individuals to cope with it might be either being more inclined to engage in privacy protection behavior, or the contrary – deeming privacy protection behaviors futile.

Third, besides the relationships explained by perceived surveillance, perceived accuracy exhibits direct positive relationships with self-empowerment, downplaying, and sympathizing, and a negative direct relationship with intention to adjust ad settings. This suggests that perceived surveillance is not the sole factor mediating this

relationship. Future research should explore other mediators that may play a contradicting role than perceived surveillance, for example, trust in the platform's competence (S. C. Chen and Dhillon 2003), which could decrease privacy protection behavior and encourage more cognitive coping strategies.

Fourth, our results revealed a conditional role for online privacy literacy in the relationship between perceived surveillance and privacy cynicism. Surprisingly, individuals with higher self-reported online privacy literacy demonstrated a stronger association between perceived surveillance and privacy cynicism, challenging our assumptions about the agency associated with privacy literacy (Masur 2020). Despite their understanding of online privacy mechanisms, individuals may still feel powerless when experiencing surveillance. The lack of significant interaction effects with other coping strategies may be due to a ceiling effect, as participants generally reported high levels of literacy. Future research should ensure a diverse sample to better understand its effects.

Last, our findings indicate a modest association between individuals' subjective evaluation of algorithmic profiling accuracy and the factual correctness of algorithmic inferences. This implies that perceived accuracy is partly based on objective accuracy, although other factors, such as pre-existing beliefs in algorithm precision, may also influence perceived accuracy (e.g., machine heuristics; Sundar and Kim 2019). Interestingly, perceived accuracy emerges as a stronger predictor of perceived surveillance and coping strategies than objective accuracy. This aligns with existing literature on perceived versus actual personalization and subjective versus objective persuasion knowledge, highlighting the greater impact of perceived accuracy on subsequent psychological responses, potentially also advertising responses (Ham and Nelson 2016; Li 2016).

References

- Bansal, Gaurav, Fatemeh “Mariam” Zahedi, and David Gefen. 2010. “The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online.” *Decision Support Systems* 49 (2): 138–50. <https://doi.org/10.1016/j.dss.2010.01.010>.
- Barbosa, Natã M., Gang Wang, Blase Ur, and Yang Wang. 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): 88:1-88:32. <https://doi.org/10.1145/3478122>.
- Bartsch, Miriam, and Tobias Dienlin. 2016. “Control Your Facebook: An Analysis of Online Privacy Literacy.” *Computers in Human Behavior* 56 (March): 147–54. <https://doi.org/10.1016/j.chb.2015.11.022>.
- Baruh, Lemi, Ekin Secinti, and Zeynep Cemalcilar. 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, Muhammad Ahmad, Umar Farooq, Maryam Shahid, Muhammad Fareed Zaffar, and Christo Wilson. 2019. “Quantity vs. Quality: Evaluating User Interest Profiles Using Ad Preference Managers.” In *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society. <https://doi.org/10.14722/ndss.2019.23392>.
- Boerman, Sophie C., Joanna Strycharz, and Edith G. Smit. 2023. “How Can We Increase Privacy Protection Behavior? A Longitudinal Experiment Testing Three Intervention Strategies.” *Communication Research*, June, 00936502231177786. <https://doi.org/10.1177/00936502231177786>.

- Brehm, Sharon S., and Jack W. Brehm. 1981. *Psychological Reactance: A Theory of Freedom and Control*. Academic Press.
- Brinöl, Pablo, Derek D. Rucker, Zakary L. Tormala, and Richard E. Petty. 2004. "Individual Differences in Resistance to Persuasion: The Role of Beliefs and Meta-Beliefs." In *Resistance and Persuasion*, edited by Eric S. Knowles and Jay A. Linn, 83–104. Mahwah, New Jersey: Lawrence Erlbaum Associates.
- Büchi, Moritz, Noemi Festic, and Michael Latzer. 2022. "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda." *Big Data & Society* 9 (1): 20539517211065368.
<https://doi.org/10.1177/20539517211065368>.
- Büchi, Moritz, Eduard Fosch-Villaronga, Christoph Lutz, Aurelia Tamò-Larrieux, and Shruthi Velidi. 2023. "Making Sense of Algorithmic Profiling: User Perceptions on Facebook." *Information, Communication & Society* 26 (4): 809–25.
<https://doi.org/10.1080/1369118X.2021.1989011>.
- Carlson, Jay P., Leslie H. Vincent, David M. Hardesty, and William O. Bearden. 2009. "Objective and Subjective Knowledge Relationships: A Quantitative Analysis of Consumer Research Findings." *Journal of Consumer Research* 35 (5): 864–76.
<https://doi.org/10.1086/593688>.
- Chen, Li, and Pearl Pu. 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, Sandy C., and Gurpreet S. Dhillon. 2003. "Interpreting Dimensions of Consumer Trust in E-Commerce." *Information Technology and Management* 4 (2): 303–18. <https://doi.org/10.1023/A:1022962631249>.

- Davis, Mark H. 1980. "A Multidimensional Approach to Individual Differences in Empathy." *JSAS Catalog of Selected Documents in Psychology* 10: 85.
- Dijk, Eric van, and Daan van Knippenberg. 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>.
- Dinev, Tamara, and Paul Hart. 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>.
- Eslami, Motahhare, Sneha R. Krishna Kumaran, Christian Sandvig, and Karrie Karahalios. 2018. "Communicating Algorithmic Process in Online Behavioral Advertising." In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. CHI '18. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/3173574.3174006>.
- Frener, Regine, Jana Dombrowski, and Sabine Trepte. 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. "My Ad Center." My Ad Center. Accessed January 11, 2024.
<https://myadcenter.google.com>.
- Ham, Chang-Dae, and Michelle R. Nelson. 2016. "The Role of Persuasion Knowledge, Assessment of Benefit and Harm, and Third-Person Perception in Coping with Online Behavioral Advertising." *Computers in Human Behavior* 62 (September): 689–702. <https://doi.org/10.1016/j.chb.2016.03.076>.
- Hautea, Samantha, Anjali Munasinghe, and Emilee Rader. 2020. "'That's Not Me': Surprising Algorithmic Inferences." In *Extended Abstracts of the 2020 CHI*

Conference on Human Factors in Computing Systems, 1–7. CHI EA '20. New York, NY, USA: Association for Computing Machinery.
<https://doi.org/10.1145/3334480.3382816>.

Hoffmann, Christian Pieter, Christoph Lutz, and Giulia Ranzini. 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>.

Jacks, Julia Zuwerink, and Kimberly A. Cameron. 2003. “Strategies for Resisting Persuasion.” *Basic and Applied Social Psychology* 25 (2): 145–61.
https://doi.org/10.1207/S15324834BASP2502_5.

Li, Cong. 2016. “When Does Web-Based Personalization Really Work? The Distinction between Actual Personalization and Perceived Personalization.” *Computers in Human Behavior* 54 (January): 25–33.
<https://doi.org/10.1016/j.chb.2015.07.049>.

Lutz, Christoph, Christian Pieter Hoffmann, and Giulia Ranzini. 2020. “Data Capitalism and the User: An Exploration of Privacy Cynicism in Germany.” *New Media & Society* 22 (7): 1168–87. <https://doi.org/10.1177/1461444820912544>.

Marwick, Alice, and Eszter Hargittai. 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, Philipp K. 2020. “How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information.” *Media and Communication* 8 (2): 258–69. <https://doi.org/10.17645/mac.v8i2.2855>.

- Masur, Philipp K., Thilo Hagendorff, and Sabine Trepte. 2023. "Challenges in Studying Social Media Privacy Literacy." In *The Routledge Handbook of Privacy and Social Media*. Routledge.
- Park, Yong Jin. 2013. "Digital Literacy and Privacy Behavior Online." *Communication Research* 40 (2): 215–36. <https://doi.org/10.1177/0093650211418338>.
- Pierce, Jon L., Tatiana Kostova, and Kurt T. Dirks. 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, Jessica, Dian A. de Vries, and Claes de Vreese. 2021. "Digital Competence across the Lifespan," June. <https://osf.io/d5c7n/>.
- Pollay, Richard W., and Banwari Mittal. 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, Pearl, Li Chen, and Rong Hu. 2012. "Evaluating Recommender Systems from the User's Perspective: Survey of the State of the Art." *User Modeling and User-Adapted Interaction* 22 (4): 317–55. <https://doi.org/10.1007/s11257-011-9115-7>.
- Rader, Emilee, Samantha Hautea, and Anjali Munasinghe. 2020. "'I Have a Narrow Thought Process': Constraints on Explanations Connecting Inferences and Self-Perceptions." In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, 457–88. SOUPS'20. USA: USENIX Association.
- Segijn, Claire M., Eunah Kim, Garim Lee, Chloe Gansen, and Sophie C. Boerman. 2023. "The Intended and Unintended Effects of Synced Advertising: When Persuasion Knowledge Could Help or Backfire." *International Journal of Research in Marketing*, July. <https://doi.org/10.1016/j.ijresmar.2023.07.001>.

- Segijn, Claire M., Eunah Kim, Asma Sifaoui, and Sophie C. Boerman. 2023. "When You Realize That Big Brother Is Watching: How Informing Consumers Affects Synced Advertising Effectiveness." *Journal of Marketing Communications* 29 (4): 317–38. <https://doi.org/10.1080/13527266.2021.2020149>.
- Segijn, Claire M., Suzanna J. Oprea, and Iris van Ooijen. 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>.
- Sifaoui, Asma. 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>.
- Strycharz, Joanna, Eunah Kim, and Claire M. Segijn. 2022. "Why People Would (Not) Change Their Media Use in Response to Perceived Corporate Surveillance." *Telematics and Informatics* 71 (July): 101838. <https://doi.org/10.1016/j.tele.2022.101838>.
- Strycharz, Joanna, and Claire M. Segijn. 2022. "The Future of Dataveillance in Advertising Theory and Practice." *Journal of Advertising* 51 (5): 574–91. <https://doi.org/10.1080/00913367.2022.2109781>.
- Sundar, S. Shyam, and Jinyoung Kim. 2019. "Machine Heuristic: When We Trust Computers More than Humans with Our Personal Information." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–9. Glasgow Scotland Uk: ACM. <https://doi.org/10.1145/3290605.3300768>.
- Voorveld, Hilde A. M., Corine S. Meppelink, and Sophie C. Boerman. 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>.

Zhang, Dong, Sophie C. Boerman, Hanneke Hendriks, Margot J. van der Goot, Theo
Araujo, and Hilde Voorveld. In press. “‘They Know Everything’: Folk Theories,
Thoughts, and Feelings about Surveillance in Media Technologies.”
International Journal of Communication.

Table 1. Measurement items and descriptive statistics

Variables (Sources)	Items/Questions	Anchors/Answer options	<i>M</i>	<i>SD</i>	α
Perceived accuracy of algorithmic profiling Self-developed; inspired by Büchi et al. (2023)	Looking at the inferences made by Google on both pages, how accurately would you say they reflect... <ul style="list-style-type: none"> Your lifestyle Your preferences Your needs and wishes Your personal characteristics You as a person 	0 = Not at all accurately 10 = Extremely accurately	5.10	2.07	.94
Perceived surveillance (Segijn, Oprea, and Ooijen 2022)	When seeing the inferences Google made about me, I felt that Google was... <ul style="list-style-type: none"> Watching my every move Checking up on me Looking over my shoulder Entering my private space 	1 = Not at all 7 = Very much	4.07	1.63	.94
Intention to adjust ad settings Self-developed; items are aligned with setting options provided in Google My Ad Center (Google, n.d.)	After seeing the inferences Google made about you, how likely would you... <ul style="list-style-type: none"> Disable certain categories/topics that Google can use for personalized ads (e.g., disallow Google from using relationship status to personalize 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 	1 = Very unlikely 7 = Very likely	4.38	1.62	.90
Privacy cynicism – resignation dimension	After seeing the inferences Google made about me, I felt that...	1 = Strongly disagree 7 = Strongly agree	3.40	1.25	.87

(Lutz, Hoffmann, and Ranzini 2020)	<ul style="list-style-type: none"> • 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)	<p>When seeing the inferences Google made about me ...</p> <ul style="list-style-type: none"> • 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 	<p>1 = Extremely unlike me</p> <p>7 = Extremely like me</p>	3.81	1.17	.91
Downplaying dataveillance cost	<p>After seeing the inferences Google made about me, I thought...</p> <ul style="list-style-type: none"> • I do not see any potential harm of Google making these inferences about me 	<p>1 = Not at all</p> <p>7 = Very much</p>	4.10	1.30	.91

(Strycharz, Kim, and Segijn 2022)	<ul style="list-style-type: none"> • 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	After seeing the inferences Google made about me...	1 = Not at all 7 = Very much	4.27	1.36	.90
Self-developed; inspired by the Perspective Taking Dimension of the Interpersonal Reactivity Index (Davis 1980)	<ul style="list-style-type: none"> • 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 - socio-demographic inferences	We asked participants to copy and paste the content of the webpage. The self-reported categories below are compared with the categories extracted from the uploaded page content. A score between 0 and 1 is calculated which indicates the percentage of correctly inferred categories out of all the available categories for each participant.		0.42	0.24	
Self-developed; items and	What is your relationship status? <ul style="list-style-type: none"> • Married • Single 				

answer		<ul style="list-style-type: none"> • In a relationship
options are		<ul style="list-style-type: none"> • Other,
aligned with		namely__
inferences		
categories	Education is computed based on two	<ul style="list-style-type: none"> • High school diploma
and options	questions about completed education and	<ul style="list-style-type: none"> • Attending college
in Google	ongoing education in the demographic	<ul style="list-style-type: none"> • Bachelor's degree
My Ad	information section of the questionnaire.	<ul style="list-style-type: none"> • Advanced degree
Center	The categories on the right side are	
(Google,	categories in Google My Ad Center	
n.d.)		
	Which industry/industries are you in?	<ul style="list-style-type: none"> • Roadworks
	Select all that apply.	<ul style="list-style-type: none"> • Education
		<ul style="list-style-type: none"> • Finance
		<ul style="list-style-type: none"> • Healthcare
		<ul style="list-style-type: none"> • Hospitality
		<ul style="list-style-type: none"> • Manufacturing
		<ul style="list-style-type: none"> • Property
		<ul style="list-style-type: none"> • Technology
		<ul style="list-style-type: none"> • Other,
		namely__
		<ul style="list-style-type: none"> • Not applicable
	What is the size of your employer? Select	<ul style="list-style-type: none"> • Small
	all that apply if you have multiple	employer (1-
	employers.	249
		employees)
		<ul style="list-style-type: none"> • Large
		employer
		(250-10,000
		employees)
		<ul style="list-style-type: none"> • Very large
		employer
		(more than

		10,000 employees)			
		• Not applicable			
	What is your home ownership situation?	• Homeowners • Renters • Other, namely__			
	What is your parenting situation?	• Not parents • Parents of infants • Parents of toddlers • Parents of preschoolers • Parents of grade schoolers • Parents of teenagers			
Objective accuracy of algorithmic profiling - interest inferences (Bashir et al. 2019)	After the participant uploads the page content, the interest inferences are parsed, and 10 interests are randomly selected. In case of errors, the participant will be asked to copy the first 10 interest inferences they see on the page one by one. Then, they are asked the following question for each inferred interest. To what extent are you interested in the following topics? The mean score of all interests indicated is computed to form a score between 1 and 7.	1 = Not at all interested 7 = Very much interested	4.18	1.15	
Online privacy literacy	To what extent do you think the following statements apply to you? Answer them as if you would have to do this activity now and without help.	1 = Completely untrue 7 = Completely true	5.54	0.97	.74

(Piotrowski, Vries, and Vreese 2021)	<p>Please be honest. It is very normal that you might not know how to do some of them.</p> <p>We would like to know how it really is for you.</p> <ul style="list-style-type: none"> • 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 <p>I know how to delete the history of websites that I have visited before</p>				
<p>Prior attitude towards personalized advertising on Google</p> <p>(Pollay and Mittal 1993)</p>	<p>Prior to participating in this study, ...</p> <ul style="list-style-type: none"> • 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 	<p>1 = Strongly disagree</p> <p>7 = Strongly agree</p>	4.07	1.37	.94
<p>Need for privacy</p> <p>(Frener, Dombrowski, and Trepte 2023)</p>	<p>In general, to what extent do you agree or disagree with the following statements?</p> <ul style="list-style-type: none"> • 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 	<p>1 = I do not agree at all</p> <p>7 = I entirely agree</p>	5.76	0.97	.86

Internet privacy concerns	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	.94
(Dinev and Hart 2006)	<ul style="list-style-type: none"> 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	When it comes to the privacy invasion of my personal data, my online experience could be characterized as:	7-point semantic differential scale	2.96	1.44	.91
(Bansal, Zahedi, and Gefen 2010)	<ul style="list-style-type: none"> 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) 				

Note. The measures are listed in the same sequence as they appeared in the questionnaire.

Table 2. Indirect, direct, and total relationships of perceived accuracy through perceived surveillance on coping strategies

Path	<i>b</i> *	(Boot) <i>SE</i>	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. Bolded coefficients represent significant relationships.

Table 3. 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. Bolded coefficients represent significant relationships.

Figure 1. Conceptual model

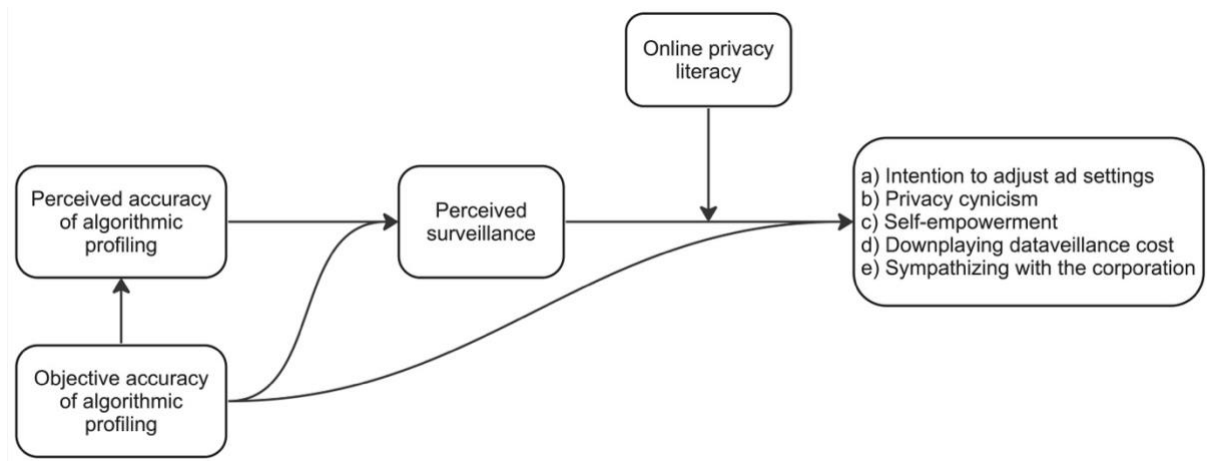


Figure 2. Relationships between perceived accuracy, perceived surveillance, online privacy literacy, and coping strategies

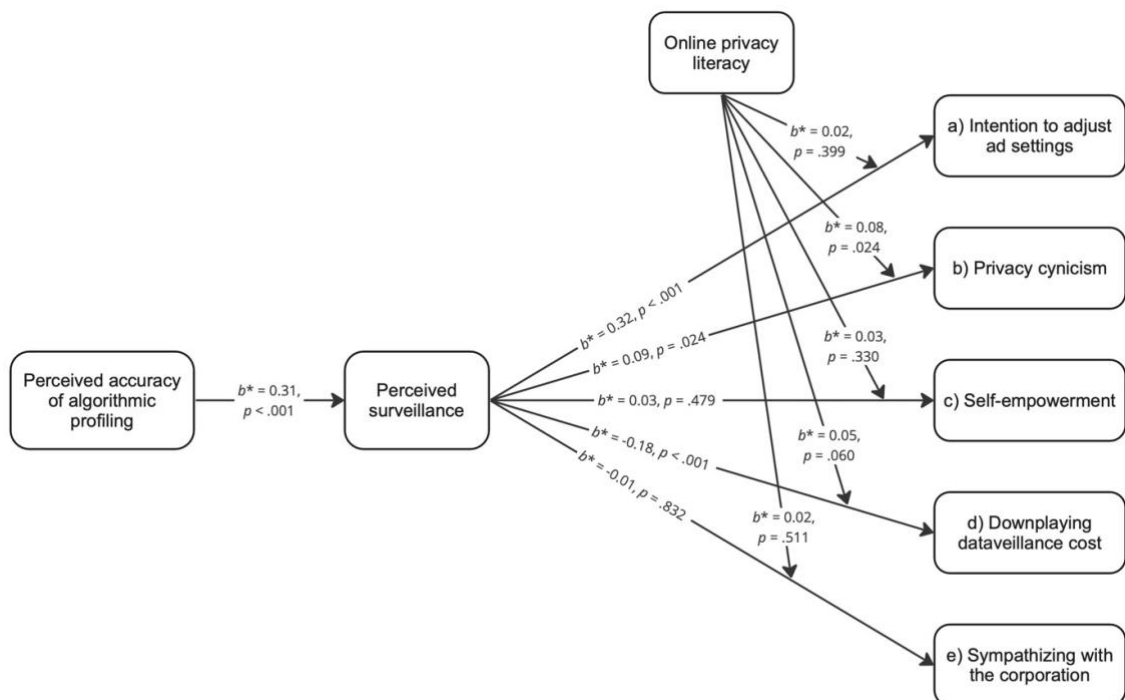


Figure 3. Interaction between perceived surveillance and online privacy literacy on privacy cynicism

