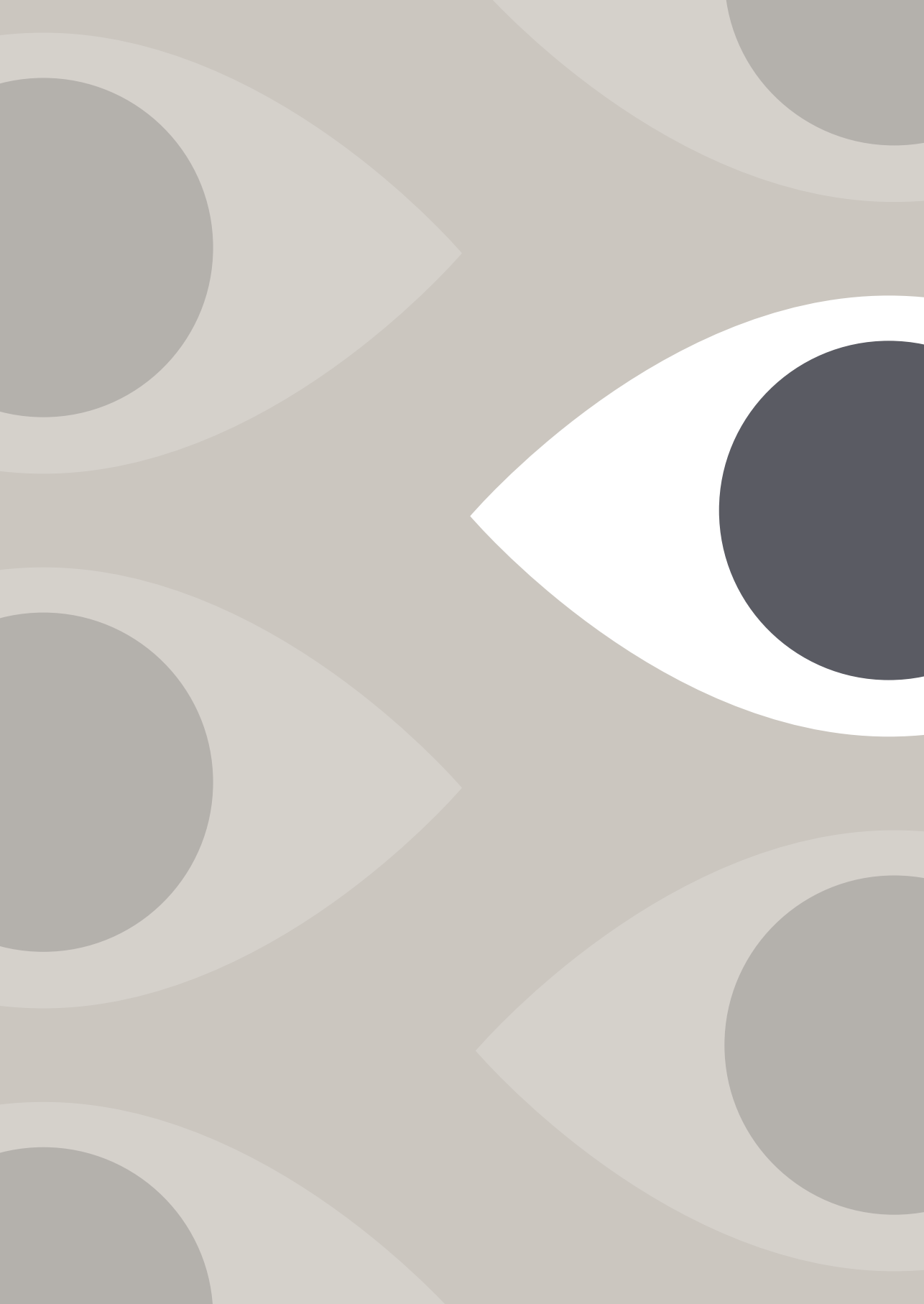
Feeling watched

Understanding triggers of and responses to perceived surveillance in digital technologies

Zhang, D.

Publication date
2026

REFERENCES



Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Conference on Electronic Commerce*, 21–29. https://doi.org/10.1145/988772.988777

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005

Amazon. (2021, February 12). *Amazon.com Privacy Notice—Amazon Customer Service*. https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ

Andrejevic, M. (2014). Big data, big questions| The big data divide. *International Journal of Communication*, *8*, 1673–1689.

Araujo, T., Boukes, M., Trilling, D., van Hoof, M., Wald, R., & Zhang, D. (2020). *Communication in the digital society survey in the Netherlands*. https://doi.org/10.17605/OSF.IO/YU64R

Arthur. (2025, January 15). *EU GDPR vs UK GDPR: Key differences explained*. https://heydata.eu/en/magazine/eu-gdpr-vs-uk-gdpr-key-differences

Augusto, F. R., & Simões, M. J. (2017). To see and be seen, to know and be known: Perceptions and prevention strategies on Facebook surveillance. *Social Science Information*, *56*(4), 596–618. https://doi.org/10.1177/0539018417734974

Baek, T. H., & Morimoto, M. (2012). Stay away from me: Examining the determinants of consumer avoidance of personalized advertising. *Journal of Advertising*, *41*(1), 59–76. https://doi.org/10.2753/JOA0091-3367410105

Bakir, V., Cable, J., Dencik, L., Hintz, A., & McStay, A. (2015). *Public feeling on privacy, security and surveillance: A report by DATA-PSST and DCSS*. https://dcssproject.net/public-feeling/

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), 88:1-88:32. https://doi.org/10.1145/3478122

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, San Diego, CA. https://doi.org/10.14722/ndss.2019.23392

Beldad, A., de Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. *The Information Society*, *27*(4), 220–232. https://doi.org/10.1080/01972243.2011.583802

Boerman, S. C., Kruikemeier, S., & Bol, N. (2021). When is personalized advertising crossing personal boundaries? How type of information, data sharing, and personalized pricing influence consumer perceptions of personalized advertising. *Computers in Human Behavior Reports*, *4*, 100144. https://doi.org/10.1016/j.chbr.2021.100144

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, *46*(3), 363–376. https://doi.org/10.1080/00913367.2017.1339368

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., & Segijn, C. M. (2022). Awareness and perceived appropriateness of synced advertising in Dutch adults. *Journal of Interactive Advertising*, *22*(2), 187–194. https://doi.org/10.1080/15252019.2022.2046216

Boerman, S. C., & Smit, E. G. (2023). Advertising and privacy: An overview of past research and a research agenda. *International Journal of Advertising*, *42*(1), 60–68. https://doi.org/10.1080/02650487.2022.2122251

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

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Bolin, G., & Jerslev, A. (2018). Surveillance through media, by media, in media. *Northern Lights: Film & Media Studies Yearbook*, *16*(1), 3–21. https://doi.org/10.1386/nl.16.1.3_2

Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. Sage.

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.

Bruder, M., Haffke, P., Neave, N., Nouripanah, N., & Imhoff, R. (2013). Measuring individual differences in generic beliefs in conspiracy theories across cultures: Conspiracy mentality questionnaire. *Frontiers in Psychology*, *4*. https://doi.org/10.3389/fpsyg.2013.00225

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, *20*(1), 30–44. https://doi.org/10.1080/1369118X.2016.1154086

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), 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*, 105367. https://doi.org/10.1016/j.clsr.2019.105367

Carver, L. F., & Mackinnon, D. (2020). Health applications of gerontechnology, privacy, and surveillance: A scoping review. *Surveillance & Society*, *18*(2), 216–230. https://doi.org/10.24908/ss.v18i2.13240

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). Sage.

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, 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, 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

Christin, A. (2020). What data can do: A typology of mechanisms. *International Journal of Communication*, *14*, 1115–1134.

Christl, W. (2017). *Corporate surveillance in everyday life: How companies collect, combine, analyze, trade, and use personal data on billions*. Cracked Labs.

Cichy, P., Salge, T. O., & Kohli, R. (2014). Extending the privacy calculus: The role of psychological ownership. *ICIS 2014 Proceedings*, *30*, 1–19.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512. https://doi.org/10.1145/42411.42413

Curran, D. (2023). Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness. *Big Data & Society*, *10*(1), 20539517231177621. https://doi.org/10.1177/20539517231177621

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

de Bruijn, G.-J., Jabeen, F., & Bosse, T. (2025). Chatbots for Mental Health. In *The Handbook of Mental Health Communication* (pp. 181–192). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781394179909.ch13

de Groot, J. I. M. (2022). The personalization paradox in Facebook advertising: The mediating effect of relevance on the personalization–brand attitude relationship and the moderating effect of intrusiveness. *Journal of Interactive Advertising*, *22*(1), 57–74. https://doi.org/10.1080/15252019.2022.2032492

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2022a). How and when personalized advertising leads to brand attitude, click, and WOM intention. *Journal of Advertising*, *51*(1), 39–56. https://doi.org/10.1080/00913367.2021.1888339

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2022b). Let's get personal: Which elements elicit perceived personalization in social media advertising? *Electronic Commerce Research and Applications*, *55*, 101183. https://doi.org/10.1016/j.elerap.2022.101183

De Keyzer, F., van Noort, G., & Kruikemeier, Sanne. (2022). Going too far? How consumers respond to personalized advertising from different sources. *Journal of Electronic Commerce Research*, *23*(3), 138–159.

Dencik, L., & Cable, J. (2017). Digital citizenship and surveillance| the advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, *11*, 763–781.

DeVito, M. A., Birnholtz, J., Hancock, J. T., French, M., & Liu, S. (2018). How people form folk theories of social media feeds and what it means for how we study self-presentation. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3173574.3173694

DeVito, M. A., Gergle, D., & Birnholtz, J. (2017). "Algorithms ruin everything": #RIPTwitter, folk theories, and resistance to algorithmic change in social media. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3163–3174. https://doi.org/10.1145/3025453.3025659

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

Dixon, S. J. (2024, July 10). *Biggest social media platforms by users 2024*. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Draper, N. A., Hoffmann, C. P., Lutz, C., Ranzini, G., & Turow, J. (2024). Privacy resignation, apathy, and cynicism: Introduction to a special theme. *Big Data & Society*, *11*(3), 20539517241270663. https://doi.org/10.1177/20539517241270663

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Duffy, B. E., & Chan, N. K. (2019). "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society*, *21*(1), 119–138. https://doi.org/10.1177/1461444818791318

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers.

Eisend, M., & Tarrahi, F. (2022). Persuasion knowledge in the marketplace: A meta-analysis. *Journal of Consumer Psychology*, *32*(1), 3–22. https://doi.org/10.1002/jcpy.1258

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. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2944243

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*, 1–13. 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*, 3029–3038. 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

Fedewa, J. (2021). *Is my smart speaker always listening to me?* How-To Geek. https://www.howtogeek.com/711565/is-my-smart-speaker-always-listening-to-me/

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, *65*, 101717. https://doi.org/10.1016/j.tele.2021.101717

Fowler, B. (2019, July 10). *Is your smartphone secretly listening to you?* Consumer Reports. https://www.consumerreports.org/smartphones/is-your-smartphone-secretly-listening-to-you/

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. (2024). Development and validation of the need for privacy scale (NFP-S). *Communication Methods and Measures*, *18*(1), 48–71. https://doi.org/10.1080/19312458.2023.2246014

Frick, N. R. J., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications*, *47*, 101046. https://doi.org/10.1016/j.elerap.2021.101046

Friestad, M., & Wright, P. (1994). The persuasion knowledge model: How people cope with persuasion attempts. *Journal of Consumer Research*, *21*(1), 1–31. https://doi.org/10.1086/209380

Fuchs, C. (2011). New media, web 2.0 and surveillance. *Sociology Compass*, *5*(2), 134–147. https://doi.org/10.1111/j.1751-9020.2010.00354.x

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.). (2012). *Internet and surveillance: The challenges of web 2.0 and social media*. Routledge. https://doi.org/10.4324/9780203806432

Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden. *Journal of Information, Communication and Ethics in Society*, *15*(4), 412–444. https://doi.org/10.1108/JICES-01-2016-0004

Gelman, S. A., & Legare, C. H. (2011). Concepts and folk theories. *Annual Review of Anthropology*, *40*(1), 379–398. https://doi.org/10.1146/annurev-anthro-081309-145822

Geuens, M., & De Pelsmacker, P. (2017). Planning and conducting experimental advertising research and questionnaire design. *Journal of Advertising*, *46*(1), 83–100. https://doi.org/10.1080/00913367.2016.1225233

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Publishing.

Gómez Ortega, A., Bourgeois, J., & Kortuem, G. (2023). What is sensitive about (sensitive) data? Characterizing sensitivity and intimacy with google assistant users. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–16. https://doi.org/10.1145/3544548.3581164

Google. (n.d.-a). *Codes and formats | Google Ads API*. Google for Developers. Retrieved March 20, 2025, from https://developers.google.com/google-ads/api/data/codes-formats

Google. (n.d.-b). *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

Google. (n.d.-c). *My Ad Center*. My Ad Center. Retrieved January 11, 2024, from https://myadcenter.google.com

Google. (2021, July 1). *Privacy Policy – Privacy & Terms – Google*. https://policies.google.com/privacy?hl=en-US

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*(CSCW1), 78:1-78:35. https://doi.org/10.1145/3512925

Guzman, A. L. (2019). Voices in and of the machine: Source orientation toward mobile virtual assistants. *Computers in Human Behavior*, *90*, 343–350. https://doi.org/10.1016/j.chb.2018.08.009

Guzman, A. L., & Lewis, S. C. (2020). Artificial intelligence and communication: A Human–Machine communication research agenda. *New Media & Society*, *22*(1), 70–86. https://doi.org/10.1177/1461444819858691

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.

Higgins, S. F., Mulvenna, M. D., Bond, R. B., McCartan, A., Gallagher, S., & Quinn, D. (2018). Multivariate testing confirms the effect of age–gender congruence on click-through rates from online social network digital advertisements. *Cyberpsychology, Behavior, and Social Networking*, *21*(10), 646–654. https://doi.org/10.1089/cyber.2018.0197

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), Article 7. https://doi.org/10.5817/CP2016-4-7

Huang, S. A., Hancock, J., & Tong, S. T. (2022). Folk theories of online dating: Exploring people's beliefs about the online dating process and online dating algorithms. *Social Media + Society*, *8*(2), 20563051221089561. https://doi.org/10.1177/20563051221089561

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication*, *61*(4), 575–595. https://doi.org/10.1111/j.1460-2466.2011.01570.x

Jacks, J. Z., & Cameron, K. A. (2003). Strategies for resisting persuasion. *Basic and Applied Social Psychology*, *25*(2), 145–161. https://doi.org/10.1207/S15324834BASP2502_5

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

Kalmus, V., Bolin, G., & Figueiras, R. (2022). Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective. *New Media & Society*, 14614448221134493. https://doi.org/10.1177/14614448221134493

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

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Kemp, S. (2024, February 21). *Digital 2024: The United Kingdom*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2024-united-kingdom

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

Kim, H., & Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising*, *38*(1), 92–105. https://doi.org/10.1080/10641734.2016.1233157

Kim, J., Zo, H., & Jun, J. (2025). How dataveillance shapes user behavior: The role of perceived value in disclosure and discontinuation. *Computers in Human Behavior*, *168*, 108655. https://doi.org/10.1016/j.chb.2025.108655

Kim, S.-Y., Levine, T. R., & Allen, M. (2017). The intertwined model of reactance for resistance and persuasive boomerang. *Communication Research*, *44*(7), 931–951. https://doi.org/10.1177/0093650214548575

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

Kozyreva, A., Lorenz-Spreen, P., Hertwig, R., Lewandowsky, S., & Herzog, S. M. (2021). Public attitudes towards algorithmic personalization and use of personal data online: Evidence from Germany, Great Britain, and the United States. *Humanities and Social Sciences Communications*, *8*, Article 117. https://doi.org/10.1057/s41599-021-00787-w

KPMG. (2023). *Responsible data use at a crossroads: European citizen's perspective on privacy*. https://kpmg.com/nl/en/home/insights/2023/12/european-privacy-market-research.html

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Kristensen, D. B., & Ruckenstein, M. (2018). Co-evolving with self-tracking technologies. *New Media & Society*, *20*(10), 3624–3640. https://doi.org/10.1177/1461444818755650

Kruikemeier, S., Boerman, S. C., & Bol, N. (2020). Breaching the contract? Using social contract theory to explain individuals' online behavior to safeguard privacy. *Media Psychology*, *23*(2), 269–292. https://doi.org/10.1080/15213269.2019.1598434

Lankton, N., McKnight, D., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10). https://doi.org/10.17705/1jais.00411

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

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, H., & Cho, C.-H. (2020). Digital advertising: Present and future prospects. *International Journal of Advertising*, *39*(3), 332–341. https://doi.org/10.1080/02650487.2019.1642015

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*, 107026. https://doi.org/10.1016/j.chb.2021.107026

Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. *Information & Management*, *55*(8), 1005–1023. https://doi.org/10.1016/j.im.2018.05.006

Lupton, D., & Michael, M. (2017). 'Depends on who's got the data': Public understandings of personal digital dataveillance. *Surveillance & Society*, *15*(2), 254–268. https://doi.org/10.24908/ss.v15i2.6332

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

Lyon, D. (2009). Surveillance, power, and everyday life. In C. Avgerou, R. Mansell, D. Quah, & R. Silverstone (Eds.), *The Oxford Handbook of Information and Communication Technologies* (1st ed., pp. 449–468). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199548798.003.0019

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Malthouse, E. C., & Li, H. (2017). Opportunities for and pitfalls of using big data in advertising research. *Journal of Advertising*, *46*(2), 227–235. https://doi.org/10.1080/00913367.2017.1299653

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), 2053951719895805. https://doi.org/10.1177/2053951719895805

Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information sensitivity and willingness to provide continua: A comparative privacy study of the United States and Brazil. *Journal of Public Policy & Marketing*, *36*(1), 79–96. https://doi.org/10.1509/jppm.15.159

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

Marx, G. T. (2015). Surveillance studies. In J. D. Wright (Ed.), *International Encyclopedia of the Social & Behavioral Sciences* (2nd ed., pp. 733–741). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Maslowska, E., Smit, E. G., & van den Putte, B. (2016). It is all in the name: A study of consumers' responses to personalized communication. *Journal of Interactive Advertising*, *16*(1), 74–85. https://doi.org/10.1080/15252019.2016.1161568

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), 258–269. https://doi.org/10.17645/mac.v8i2.2855

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.

McEwan, B., & Flood, M. (2018). Passwords for jobs: Compression of identity in reaction to perceived organizational control via social media surveillance. *New Media & Society*, *20*(5), 1715–1734. https://doi.org/10.1177/1461444817706073

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, *2*(2), 12:1-12:25. https://doi.org/10.1145/1985347.1985353

Meaker, M. (2024, October 4). *Meta can't use sexual orientation to target ads in the EU, court rules*. Wired. https://www.wired.com/story/meta-cant-use-sexual-orientation-to-target-ads-in-the-eu-court-rules/

Meier, Y., Oeldorf-Hirsch, A., & Krämer, N. C. (2024). Who is targeting me? Privacy perceptions of and responses to commercial and political targeted advertising on social media. *Journal of Advertising*, *53*(4), 473–490. https://doi.org/10.1080/00913367.2023.2275776

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

Meng, X. (2024). Conceptualizing and measuring privacy boundary turbulence in technological contexts: Constructing a measurement scale. *Information Processing & Management*, *61*(3), 103658. https://doi.org/10.1016/j.ipm.2024.103658

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

Meta. (n.d.-b). *Targeting Search—Marketing API - Documentation*. Meta for Developers. Retrieved March 20, 2025, from https://developers.facebook.com/docs/marketing-api/audiences/reference/targeting-search/

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

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

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 1–21. https://doi.org/10.1177/2053951716679679

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research*, *15*(1), 76–98. https://doi.org/10.1177/1094670511424924

Ohme, J., Araujo, T., Boeschoten, L., Freelon, D., Ram, N., Reeves, B. B., & Robinson, T. N. (2024). Digital trace data collection for social media effects research: APIs, data donation, and (screen) tracking. *Communication Methods and Measures*, *18*(2), 124–141. https://doi.org/10.1080/19312458.2023.2181319

Orlowski, J. (Director). (2020). *The Social Dilemma* [Video recording]. Netflix.

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

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Sage.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=103660

Phelan, C., Lampe, C., & Resnick, P. (2016). It's creepy, but it doesn't bother me. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5240–5251. https://doi.org/10.1145/2858036.2858381

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., de Vries, D., de Vreese, C., van Oosten, A., & Korderijnk, R. (2021). *Digital competence across the lifespan*. https://osf.io/d5c7n/

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive Marketing*, *50*, 32–44. https://doi.org/10.1016/j.intmar.2019.10.004

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 Usable Privacy and Security*, 457–488.

Raehsler, L. (2025, February 12). *Layering success: How to target high-intent users in google ads*. Search Engine Journal. https://www.searchenginejournal.com/layering-success-target-high-intent-users-in-google-ads/536347/

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

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Pub. L. No. 32016R0679, 119 OJ L (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (United Kingdom General Data Protection Regulation) (Text with EEA Relevance) (2016). https://www.legislation.gov.uk/eur/2016/679

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance), 277 OJ L (2022). http://data.europa.eu/eli/reg/2022/2065/oj/eng

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

Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24. https://doi.org/10.1080/17530350.2019.1574866

Rumbold, J. M. M., & Pierscionek, B. K. (2018). What are data? A categorization of the data sensitivity spectrum. *Big Data Research*, *12*, 49–59. https://doi.org/10.1016/j.bdr.2017.11.001

Saravanos, A., Zervoudakis, S., Zheng, D., Nanda, A., Shaheen, G., Hornat, C., Konde Chaettle, J., Yoda, A., Park, H., & Ang, W. (2022). Reputation, risk, and trust on user adoption of internet search engines: The case of DuckDuckGo. In C. Stephanidis, M. Antona, S. Ntoa, & G. Salvendy (Eds.), *HCI International 2022 – Late Breaking Posters* (pp. 683–691). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-19679-9_87

Scheiber, N. (2017, April 2). How Uber uses psychological tricks to push its drivers' buttons. *The New York Times*. https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html

Schomakers, E.-M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. *International Journal of Information Management*, *46*, 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Segijn, C. M., Kim, E., Lee, G., Gansen, C., & Boerman, S. C. (2024). The intended and unintended effects of synced advertising: When persuasion knowledge could help or backfire. *International Journal of Research in Marketing*, *41*(1), 156–169. 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., Kim, E., & van Ooijen, I. (2024). The role of perceived surveillance and privacy cynicism in effects of multiple synced advertising exposures on brand attitude. *Journal of Current Issues & Research in Advertising*, *45*(4), 506–522. https://doi.org/10.1080/10641734.2024.2318711

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), Article 9. https://doi.org/10.5817/CP2022-3-9

Segijn, C. M., Strycharz, J., Riegelman, A., & Hennesy, C. (2021). A literature review of personalization transparency and control: Introducing the transparency–awareness–control framework. *Media and Communication*, *9*(4), 120–133. https://doi.org/10.17645/mac.v9i4.4054

Segijn, C. M., Strycharz, J., Turner, A., & Opree, S. J. (2024). Conversation-related advertising and electronic eavesdropping: Mapping perceptions of phones listening for advertising in the United States, the Netherlands, and Poland. *Social Media + Society*, *10*(4), 20563051241288448. https://doi.org/10.1177/20563051241288448

Segijn, C. M., Strycharz, J., Turner, A., & Opree, S. J. (2025). "My phone must be listening!": Peoples' surveillance beliefs around devices "listening" to offline conversations in the US, the Netherlands, and Poland. *Big Data & Society*, *12*(2), 20539517251337102. https://doi.org/10.1177/20539517251337102

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

Segijn, C. M., & van Ooijen, I. (2022). Differences in consumer knowledge and perceptions of personalized advertising: Comparing online behavioural advertising and synced advertising. *Journal of Marketing Communications*, *28*(2), 207–226. https://doi.org/10.1080/13527266.2020.1857297

Segijn, C. M., van Ooijen, I., & Opree, S. J. (2020). *The validation of the perceived surveillance scale*. 71st Annual ICA Conference.

Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. *Social and Personality Psychology Compass*, *10*(9), 503–518. https://doi.org/10.1111/spc3.12265

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

Sifaoui, A., & Segijn, C. M. (2025). Surveillance in the advertising landscape: Application of the DEAL framework to investigate online behavioral advertising, surveillance, and users' responses on instagram. *Journal of Current Issues & Research in Advertising*, *46*(4), 524–538. https://doi.org/10.1080/10641734.2024.2419602

Siles, I., Segura-Castillo, A., Solís, R., & Sancho, M. (2020). Folk theories of algorithmic recommendations on Spotify: Enacting data assemblages in the global South. *Big Data & Society*, *7*(1), 2053951720923377. https://doi.org/10.1177/2053951720923377

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

Smit, E. G., van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745.

Spears, N., & Singh, S. N. (2004). Measuring attitude toward the brand and purchase intentions. *Journal of Current Issues & Research in Advertising*, *26*(2), 53–66. https://doi.org/10.1080/10641734.2004.10505164

Squires, A. (2009). Methodological challenges in cross-language qualitative research: A research review. *International Journal of Nursing Studies*, *46*(2), 277–287. https://doi.org/10.1016/j.ijnurstu.2008.08.006

Stanton, J. M., & Stam, K. R. (2003). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance & Society*, *1*(2), 152–190. https://doi.org/10.24908/ss.v1i2.3351

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*, 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), Article 1. https://doi.org/10.5817/CP2019-2-1

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., & Segijn, C. M. (2024). Ethical side-effect of dataveillance in advertising: Impact of data collection, trust, privacy concerns and regulatory differences on chilling effects. *Journal of Business Research*, *173*, 114490. https://doi.org/10.1016/j.jbusres.2023.114490

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*, 106750. https://doi.org/10.1016/j.chb.2021.106750

Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019). Consumer view on personalized advertising: Overview of self-reported benefits and concerns. In E. Bigne & S. Rosengren (Eds.), *Advances in Advertising Research X: Multiple Touchpoints in Brand Communication* (pp. 53–66). Springer Fachmedien. https://doi.org/10.1007/978-3-658-24878-9_5

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*, 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*, 1–9. https://doi.org/10.1145/3290605.3300768

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1410

Tidy, J. (2019, September 5). Why phones that secretly listen to us are a myth. *BBC News*. https://www.bbc.com/news/technology-49585682

Torkamaan, H., Barbu, C.-M., & Ziegler, J. (2019). How can they know that? A study of factors affecting the creepiness of recommendations. *Proceedings of the 13th ACM Conference on Recommender Systems*, 423–427. https://doi.org/10.1145/3298689.3346982

Turow, J. (2021). *The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet*. Yale University Press.

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 Usable Privacy and Security*, 1–15. https://doi.org/10.1145/2335356.2335362

Valkenburg, P. M., & Peter, J. (2013). The differential susceptibility to media effects model. *Journal of Communication*, *63*(2), 221–243. https://doi.org/10.1111/jcom.12024

van Berlo, Z. M. C., Sungur, H., & Gyarmati, F. M. (2025). Learning in virtual reality: The relationship between cognitive load, interactivity, and learning outcomes. *Journal of Media Psychology*. https://econtent.hogrefe.com/doi/10.1027/1864-1105/a000460

van Deursen, A. J. A. M., Helsper, E. J., & Eynon, R. (2016). Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society*, *19*(6), 804–823. https://doi.org/10.1080/1369118X.2015.1078834

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001

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

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2022). Privacy cynicism and its role in privacy decision-making. *Communication Research*, 00936502211060984. https://doi.org/10.1177/00936502211060984

van Reijmersdal, E. A., Fransen, M. L., van Noort, G., Opree, S. J., Vandeberg, L., Reusch, S., van Lieshout, F., & Boerman, S. C. (2016). Effects of disclosing sponsored content in blogs: How the use of resistance strategies mediates effects on persuasion. *American Behavioral Scientist*, *60*(12), 1458–1474. https://doi.org/10.1177/0002764216660141

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763. https://doi.org/10.1016/j.chb.2021.106763

Voorveld, H. A. M., Meppelink, C. S., & Boerman, S. C. (2024). Consumers' persuasion knowledge of algorithms in social media advertising: Identifying consumer groups based on awareness, appropriateness, and coping ability. *International Journal of Advertising*, *43*(6), 960–986. 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

Voorveld, H. A. M., Segijn, C. M., Ketelaar, P. E., & Smit, E. G. (2014). Investigating the prevalence and predictors of media multitasking across countries. *International Journal of Communication*, *8*, 2755–2777.

Wang, L. H., Metzger, M. J., Liu, X., & Li Qi. (2025). Seeing ad transparency more clearly: Public perception, use of ad transparency tools, and responses to dataveillance. *Journal of Advertising*, *54*(2), 213–232. https://doi.org/10.1080/00913367.2025.2451993

Ytre-Arne, B., & Moe, H. (2021). Folk theories of algorithms: Understanding digital irritation. *Media, Culture & Society*, *43*(5), 807–824. https://doi.org/10.1177/0163443720972314

Zhang, D., Boerman, S. C., Hendriks, H., Araujo, T., & Voorveld, H. (2023). A peek 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. (2022). *"They know everything": Folk theories, thoughts, and feelings about surveillance in media technologies*. 72nd Annual ICA Conference, Paris, France.

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.

Zhang, D., Strycharz, J., Boerman, S. C., Araujo, T., & Voorveld, H. (2025). Google knows me too well! Coping with perceived surveillance in an algorithmic profiling context. *Computers in Human Behavior*, *165*, 108536. https://doi.org/10.1016/j.chb.2024.108536

Zhang, D., Voorveld, H., & Boerman, S. C. (2023). Privacy concerns matter, knowledge does not: Investigating effects of online behavioral advertising among Chinese and Dutch adults. *Journal of Current Issues & Research in Advertising*, *44*(3), 392–410. https://doi.org/10.1080/10641734.2023.2199812

Zhao, L. (2023). Filter bubbles? Also protector bubbles! Folk theories of Zhihu algorithms among Chinese gay men. *Social Media + Society*, *9*(2), 20563051231168647. https://doi.org/10.1177/20563051231168647

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (1st ed.). PublicAffairs.

ENGLISH SUMMARY

With digital technologies seeping through people's everyday lives, more and more personal data are being collected, stored, and processed to regulate or govern the behavior of individuals or groups, a phenomenon known as dataveillance. For each individual living in a digital society, while it is simply impossible to keep track of every instance of data collection, there are almost certainly some experiences where they become aware of, or assume, that their data are being collected. These experiences trigger perceived surveillance—the feeling of being watched, listened to, or having one's data recorded. This dissertation seeks to understand this feeling of perceived surveillance by investigating individuals' beliefs surrounding it, what triggers it, how it influences individuals' coping and message responses, and which individual differences and technological contexts relate to it.

DISSERTATION AIMS

This dissertation had four research aims. These aims set out to address four key research gaps in the current understanding of perceived surveillance.

1. **To map individuals' beliefs about dataveillance:**

   This aim involved exploring how people conceptualize dataveillance (who they think is surveilling them, for what purposes, and how) and their evaluations of these practices (their positive and negative thoughts and feelings).

2. **To examine the specific triggers of perceived surveillance:**

   This aim focused on what precisely causes the feeling of being surveilled when individuals notice that their data are being collected. This included investigating the role of perceived and objective accuracy of algorithmic profiling, as well as the sensitivity and amount of data used in data-driven advertising.

3. **To investigate the consequences of perceived surveillance for individuals' coping strategies and responses to data-driven advertising:**

   This aim revolved around understanding how feeling surveilled impacts the adoption of coping strategies like privacy protection intention and privacy cynicism among individuals, as well as how it influences their attitudes toward ads, brands, and platforms when dataveillance is used for data-driven advertising.

4. **To explore individual differences and contextual factors related to perceived surveillance:**

This aim sought to investigate whether the level of perceived surveillance varies significantly among different individuals (e.g., based on age, education, privacy concerns) and across various technological contexts (e.g., social media, smart devices).

The dissertation employed four empirical studies. The first study (Chapter 2) reported in-depth interviews with 23 Dutch adults, focusing on their folk theories, thoughts, and feelings about dataveillance in digital technologies. The second study (Chapter 3) was a cross-sectional survey with a representative sample of 1,994 Dutch adults, quantitatively describing perceived sources and purposes of surveillance, and investigating individual differences and technological contexts related to perceived surveillance. The third study (Chapter 4) utilized a cross-sectional survey, asking 685 adults in the United Kingdom (UK) to view their actual algorithmic profiles from Google, examining how perceived and objective accuracy of algorithmic profiling relate to perceived surveillance and different coping strategies. The fourth study (Chapter 5) was an online experiment with 1,256 UK adults, investigating how the sensitivity and amount of data in data-driven advertisements influence perceived surveillance and its consequences on advertising effectiveness and privacy cynicism.

MAIN CONCLUSIONS

Together, the studies presented in this dissertation provide six key findings:

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

The dissertation identified various conceptualizations of dataveillance, forming folk theories based on perceived sources (who is surveilling), purposes (why are they surveilling), and mechanisms (how do they surveil). The most prominent folk theory is that *companies do everything to collect data for money*. This perception is primarily driven by individuals' experiences with data-driven advertising, as quantitative findings in the Dutch population showed that advertisers are perceived as the main sources of dataveillance, with advertising being the main perceived purpose. Compared to state surveillance or other forms of surveillance, corporate surveillance, particularly for advertising purposes, is perceived as far more pervasive in daily digital experiences. Individuals' beliefs align with the concept of surveillance capitalism, indicating awareness of corporations' profit-making goals. Furthermore, technologies are perceived as direct dataveillance sources but ultimately controlled by companies, offering a nuanced understanding of their role in dataveillance.

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

Individuals hold mixed views about dataveillance. On the one hand, they acknowledge the benefits, such as improved user experience, benefits extending beyond technology (e.g., health improvements), and a general appreciation for the "smartness" of these systems. On the other hand, people perceive a power imbalance between themselves and data collectors, have concerns over unethical practices and privacy, feel violated, and find it creepy. This finding extends the privacy calculus model by incorporating affective dimensions like feelings of violation and creepiness as perceived costs.

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

Perceived surveillance is triggered when people observe instances of data collection, such as viewing algorithmic profiles or seeing data-driven ads. The specific features of these instances also matter. When individuals see their own algorithmic profiles, both perceived and objective accuracy of algorithmic profiling are positively related to perceived surveillance: the more accurate a profile is, the more surveilled individuals feel. In the context of data-driven advertising, ads using highly sensitive data (e.g., income, location) or multiple types of data evoke higher perceived surveillance than ads using less sensitive (e.g., gender, age) or a single type of data. Notably, using high-sensitivity data triggers the strongest perceived surveillance regardless of data amount, suggesting that data sensitivity plays a more critical role in eliciting perceived surveillance. This finding contributes to current knowledge by integrating multiple theories to explain how specific characteristics of data or the outcome of data collection can lead to varying degrees of perceived surveillance and providing valuable empirical evidence.

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

To cope with heightened feelings of perceived surveillance, people increase their intentions to protect their privacy (e.g., through adjusting ad settings). Another potential coping strategy is privacy cynicism, a feeling that privacy protection is futile. The relationship between perceived surveillance and privacy cynicism, however, showed varied results, suggesting that only impactful personal experiences might be able to change the levels of privacy cynicism among individuals. While this dissertation also qualitatively identified other coping strategies like self-empowerment, downplaying dataveillance cost, and sympathizing with the corporation, these strategies are not directly and positively associated with perceived surveillance. Instead, they are directly

related to the perceived accuracy of algorithmic profiling, suggesting other mechanisms like trust and surprise might exist. These findings revealed and examined these distinct coping strategies individuals adopt in response to dataveillance, contributing to our understanding of how people cognitively manage the tension between awareness of dataveillance and continued digital engagement.

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

Another consequence of perceived surveillance is its negative impact on individuals' ad responses. When individuals feel surveilled due to seeing data-driven advertising, they develop more negative attitudes not only toward the ad and the brand, but also toward the platform on which the ad is displayed (e.g., social media platforms). This expands previous research that mostly focused on ad and brand evaluations by showing that individuals can develop negative attitudes toward any party that is perceived as involved in dataveillance practices when personal data are used in persuasive messages. It also challenges the notion of platforms as neutral channels, suggesting that people do hold platforms accountable for dataveillance practices that enable data-driven advertising.

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

Perceived surveillance is related to several individual differences. It is positively associated with privacy concerns and conspiracy mentality. Younger and highly educated individuals tend to perceive higher levels of surveillance. Additionally, online privacy literacy moderates the relationship between perceived surveillance and privacy cynicism. Furthermore, the technological context also plays a role, with social media and web browsers perceived as most surveilling, and smart watches and smart home devices as least surveilling. This finding empirically supports the proposition that individual differences and contextual factors shape responses to dataveillance, contributing to our understanding of who is most susceptible to feeling surveilled and in which contexts people are more likely to experience this perception.

PRACTICAL IMPLICATIONS

This dissertation offers actionable insights for advertisers, ad platforms, and policymakers and regulators. For advertisers, there is a critical need to balance ad personalization benefits with the drawbacks of triggering perceived surveillance. It is recommended to carefully select the type and amount of data used for personalization,

especially avoiding too sensitive (e.g., personal income, current location, search history, browsing history, mental health) or extensive types of data. Following these recommendations can help mitigate heightened perceived surveillance and negative attitudes toward ads, brands, and platforms.

For ad platforms, making accurate algorithmic profiles about users might lead to individuals adopting more privacy protection behavior, consequently limiting future possibilities of data collection. Users also develop negative attitudes toward the platform when it delivers ads using too sensitive data or multiple types of data. It is recommended to be more selective with the collection and use of data, adopt more responsible data practices, and provide users with more meaningful, visible, and easy-to-use control options.

For policymakers and regulators, the findings suggest that current regulations might need to be expanded to include a broader list of special category data, as many data types commonly used for advertising (e.g., location, search history) are considered highly sensitive by consumers but are not yet recognized or protected as special category data under current regulations. Regulations should also require full disclosure of all data used for advertising, not just "main parameters" to enable informed consumer decisions. Additionally, it is recommended to further limit the scope of dataveillance and ensure accessible privacy protection tools to counter privacy cynicism and empower users.

OVERALL CONCLUSION

Overall, this dissertation provides insights into individuals' beliefs about dataveillance, the triggers and consequences of perceived surveillance, and individual and contextual factors related to perceived surveillance. It concludes that corporate surveillance is a main driver of the perceptions of surveillance among individuals, and individuals see both benefits and costs of being surveilled. In instances where one observes data collection, the sensitivity of data, amount of data, and the accuracy of inferences made from the data can heighten perceived surveillance. Subsequently, individuals cope with this feeling with increased privacy protection intention but potentially also privacy cynicism. Furthermore, feeling surveilled as a result of seeing data-driven advertising damages individuals' attitudes toward the ad, the brand, and the platform. Lastly, perceived surveillance also varies with individual differences and technological contexts.

NEDERLANDSE SAMENVATTING

Nu het dagelijks leven van mensen steeds meer doordrongen raakt van digitale technologieën, worden ook steeds meer persoonsgegevens verzameld, opgeslagen en verwerkt. Deze worden gebruikt om het gedrag van individuen of groepen te reguleren of sturen, een fenomeen dat bekendstaat als *dataveillance*. Voor een individu in een digitale samenleving, is het simpelweg onmogelijk om elke keer dat gegevens worden verzameld bij te houden. Tegelijkertijd maakt ieder individu wel situaties mee waarin men zich ervan bewust wordt, of veronderstelt, dat gegevens over hen worden verzameld. Deze ervaringen roepen *perceived surveillance* op: het gevoel dat men bekeken of beluisterd wordt, of dat iemands gegevens worden vastgelegd. Dit proefschrift probeert dit gevoel van *perceived surveillance* te begrijpen door te onderzoeken welke overtuigingen individuen hierover hebben, wat dit gevoel oproept of triggert, hoe het beïnvloedt hoe mensen reageren op (respons) en omgaan met boodschappen (coping), en welke individuele verschillen en technologische contexten hiermee samenhangen.

DOELSTELLINGEN VAN HET PROEFSCHRIFT

Dit proefschrift had vier doelen. Deze doelen beoogden vier belangrijke hiaten in de literatuur over het huidige begrip van *perceived surveillance* te adresseren.

1. **De opvattingen van individuen over dataveillance in kaart brengen:**

   Dit doel betrof het verkennen van hoe mensen dataveillance conceptualiseren (wie zij denken dat hun gegevens verzamelt, met welke doeleinden en hoe) en hoe zij deze praktijken evalueren (hun positieve en negatieve gedachten en gevoelens).

2. **De specifieke triggers van perceived surveillance onderzoeken:**

   Dit doel richtte zich op de oorzaken of triggers van perceived surveillance: wat zorgt er nu voor dat dit gevoel wordt opgeroepen? Dit omvatte het onderzoeken van de rol van de waargenomen en objectieve nauwkeurigheid van algoritmische profilering, evenals de gevoeligheid en de hoeveelheid gegevens die worden gebruikt bij datagedreven adverteren.

3. **De consequenties van perceived surveillance voor copingstrategieën en reacties op datagedreven advertenties onderzoeken:**

   Dit doel draaide om het begrijpen van hoe het gevoel gesurveilleerd te worden de inzet van copingstrategieën, zoals de intentie om de privacy te beschermen en privacy cynisme, beïnvloedt, evenals hoe dit attitudes ten aanzien van advertenties, merken en platforms beïnvloedt wanneer dataveillance wordt ingezet voor datagedreven advertenties.

4. **Individuele verschillen en contextuele factoren die samenhangen met perceived surveillance verkennen:**

   Dit doel beoogde te onderzoeken of de mate van perceived surveillance significant verschilt tussen individuen (bijv. op basis van leeftijd, opleiding, ongerustheid over privacy) en tussen verschillende technologische contexten (bijv. sociale media, slimme apparaten).

Het proefschrift omvatte vier empirische studies. De eerste studie (Hoofdstuk 2) rapporteerde diepte-interviews met 23 Nederlandse volwassenen en richtte zich op hun lekentheorieën (persoonlijke, intuïtieve overtuigen van mensen die zij vormen op basis van eigen ervaringen en observaties, zonder formele wetenschappelijke kennis), gedachten en gevoelens over dataveillance in digitale technologieën. De tweede studie (Hoofdstuk 3) was een cross-sectionele survey onder een representatieve steekproef van 1.994 Nederlandse volwassenen, die kwalitatief beschreef door wie mensen denken dat hun gegevens verzameld wordt en met welke doeleinden. Ook beschreef de studie individuele verschillen en technologische contexten in relatie tot perceived surveillance. De derde studie (Hoofdstuk 4) maakte gebruik van een cross-sectionele survey, waarbij 685 volwassenen in het Verenigd Koninkrijk hun eigen algoritmische profielen van Google te zien kregen, waarbij onderzocht werd hoe de waargenomen en objectieve nauwkeurigheid van algoritmische profilering samenhangen met perceived surveillance en verschillende copingstrategieën. De vierde studie (Hoofdstuk 5) was een online experiment met 1.256 volwassenen in het Verenigd Koninkrijk, waarin is onderzocht hoe de gevoeligheid en de hoeveelheid gegevens die gebruikt worden in datagedreven advertenties de perceived surveillance beïnvloeden en welke gevolgen dit heeft voor reclame-effectiviteit en privacy cynisme.

BELANGRIJKSTE CONCLUSIES

Gezamenlijk leveren de studies die beschreven worden in dit proefschrift zes kernbevindingen op:

Kernbevinding 1: Datagedreven adverteren staat centraal in de belangrijkste lekentheorie "bedrijven doen alles om gegevens te verzamelen voor geld"

Het proefschrift identificeerde verschillende conceptualisaties van dataveillance, die zich uiten in de lekentheorieën die mensen vormen op basis van wie zij denken dat hun gegevens verzameld (bronnen), waarom hun gegevens verzameld worden (doelen) en op wat voor manieren dat gebeurt (mechanismen). De meest voorkomende lekentheorie is

dat "bedrijven alles doen om gegevens te verzamelen voor geld." Deze perceptie wordt primair gedreven door ervaringen met datagedreven advertenties, aangezien kwantitatieve bevindingen in de Nederlandse bevolking laten zien dat adverteerders als de belangrijkste bronnen van dataveillance worden gezien, terwijl adverteren als het belangrijkste doel wordt gezien. In vergelijking met staatssurveillance of andere vormen van surveillance wordt surveillance door bedrijven, met name voor advertentiedoeleinden, ervaren als veel meer doordrongen van dagelijkse digitale ervaringen. De overtuigingen van individuen sluiten aan bij het concept van surveillancekapitalisme en duiden op een bewustzijn van de winstmotieven van bedrijven. Bovendien worden technologieën gezien als directe bronnen van dataveillance, maar die uiteindelijk gecontroleerd worden door bedrijven, wat een genuanceerd begrip biedt van hun rol binnen dataveillance.

Kernbevinding 2: Mensen zien zowel voordelen als kosten van dataveillance

Mensen hebben gemengde opvattingen over dataveillance. Enerzijds erkennen zij voordelen, zoals een verbeterde gebruikerservaring, voordelen die verder reiken dan technologie (bijv. gezondheidsverbeteringen) en een algemene waardering voor de 'slimheid' van deze systemen. Anderzijds ervaren mensen een disbalans in macht tussen henzelf en de verzamelaars van de gegevens, maken zij zich zorgen over onethische praktijken en privacy, voelen zij zich geschonden en vinden zij het 'creepy'. Deze bevinding breidt het privacy-calculatiemodel uit door affectieve dimensies, zoals gevoelens van privacyschending en 'creepiness', als nadelen die ervaren worden op te nemen.

Kernbevinding 3: Nauwkeurigheid van algoritmische profilering en de gevoeligheid en hoeveelheid gegevens die worden gebruikt bij datagedreven adverteren beïnvloeden perceived surveillance

Perceived surveillance wordt getriggerd wanneer mensen gegevensverzameling opmerken, zoals het bekijken van algoritmische profielen of het zien van datagedreven advertenties. De specifieke kenmerken van deze gegevensverzameling doen er ook toe. Wanneer individuen hun eigen algoritmische profielen zien, hangen zowel de waargenomen als de objectieve nauwkeurigheid van algoritmische profilering positief samen met perceived surveillance: hoe nauwkeuriger een profiel is, des te sterker men zich gesurveilleerd voelt. In de context van datagedreven adverteren roepen advertenties die zeer gevoelige gegevens gebruiken (bijv. inkomen, locatie) of meerdere soorten gegevens inzetten, een hogere perceived surveillance op dan advertenties die minder gevoelige (bijv. gender, leeftijd) of slechts één type gegevens gebruiken. Opvallend is dat het gebruik van zeer gevoelige gegevens de sterkste perceived surveillance oproept, ongeacht de hoeveelheid gegevens, wat suggereert dat de gevoeligheid van gegevens

een crucialere rol speelt bij het oproepen van perceived surveillance. Deze bevinding draagt bij aan de huidige kennis door meerdere theorieën te integreren om te verklaren hoe specifieke kenmerken van gegevens of de resultaten van de gegevensverzameling kunnen leiden tot uiteenlopende gradaties van perceived surveillance en levert waardevol empirisch bewijs.

Kernbevinding 4: Om met perceived surveillance om te gaan ontwikkelen mensen enerzijds een sterkere intentie om de privacy te beschermen, maar anderzijds ook een hoger privacy cynisme

Om te kunnen omgaan met verhoogde gevoelens van perceived surveillance, vergroten mensen hun intenties om hun privacy te beschermen (bijv. door advertentie-instellingen aan te passen). Een andere mogelijke copingstrategie is privacy cynisme: het gevoel dat privacybescherming zinloos is. De relatie tussen perceived surveillance en privacy cynisme liet echter uiteenlopende resultaten zien, wat suggereert dat alleen ingrijpende persoonlijke ervaringen de mate van privacy cynisme bij individuen kunnen veranderen. Hoewel dit proefschrift in het kwalitatieve onderzoek ook andere copingstrategieën identificeerde, zoals self-empowerment, het bagatelliseren van de kosten van dataveillance en het sympathiseren met het bedrijf, hangen deze strategieën niet direct en positief samen met perceived surveillance. Ze hangen in plaats daarvan direct samen met de waargenomen nauwkeurigheid van algoritmische profilering, wat op andere mechanismen kan wijzen, zoals vertrouwen en verrassing. Deze bevindingen onthullen en onderzoeken de afzonderlijke copingstrategieën die individuen hanteren in reactie op dataveillance, en dragen bij aan ons begrip van hoe mensen cognitief omgaan met de spanning tussen het bewustzijn van dataveillance en het willen blijven gebruiken van digitale technologieën.

Kernbevinding 5: Perceived surveillance schaadt attitudes ten opzichte van de advertentie, het merk en het platform

Een andere consequentie van perceived surveillance is de negatieve impact op hoe individuen op advertenties reageren. Wanneer mensen zich gesurveilleerd voelen door het zien van datagedreven advertenties, ontwikkelen zij negatievere attitudes, niet alleen ten opzichte van de advertentie en het merk, maar ook ten opzichte van het platform waarop de advertentie wordt getoond (bijv. sociale-mediaplatforms). Dit breidt eerder onderzoek, dat vooral focuste op evaluaties van advertentie en merk, uit door te laten zien dat individuen negatieve attitudes kunnen ontwikkelen tegenover elke partij die als betrokken wordt gezien bij dataveillance-praktijken wanneer persoonsgegevens worden gebruikt in persuasieve boodschappen. Het daagt ook de opvatting uit dat platforms

slechts neutrale kanalen zijn en suggereert dat mensen platforms wél verantwoordelijk houden voor dataveillance-praktijken die datagedreven advertenties mogelijk maken.

Kernbevinding 6: Perceived surveillance varieert met individuele verschillen en technologische contexten

Perceived surveillance hangt samen met verschillende individuele verschillen. Het is positief geassocieerd met ongerustheid over privacy en complotmentaliteit. Jongere en hoogopgeleide individuen ervaren doorgaans hogere niveaus van surveillance. Daarnaast modereert online privacygeletterdheid de relatie tussen perceived surveillance en privacy cynisme. Ook de technologische context speelt een rol: bij sociale media en webbrowsers wordt surveillance het sterkst ervaren, terwijl dit bij smartwatches en smarthome-apparaten veel minder is. Deze bevinding biedt empirische ondersteuning voor de stelling dat individuele verschillen en contextuele factoren de reacties op dataveillance vormgeven en draagt bij aan ons begrip van wie het meest vatbaar is voor het gevoel gesurveilleerd te worden en in welke contexten mensen dit gevoel met name ervaren.

PRAKTISCHE IMPLICATIES

Dit proefschrift biedt toepasbare inzichten voor adverteerders, advertentieplatforms en beleidsmakers en toezichthouders. Voor adverteerders is er een cruciale noodzaak om de voordelen van het personaliseren van advertenties in balans te brengen met de nadelen van perceived surveillance. Er wordt aanbevolen om zorgvuldig het type en de hoeveelheid gegevens te selecteren die voor personalisatie worden gebruikt, en met name te vermijden dat te gevoelige (bijv. persoonlijk inkomen, huidige locatie, zoekgeschiedenis, browsegeschiedenis, mentale gezondheid) of te veel soorten gegevens worden ingezet. Het volgen van deze aanbevelingen kan helpen om verhoogde perceived surveillance en negatieve attitudes ten opzichte van advertenties, merken en platforms te verminderen.

Voor advertentieplatforms geldt dat het opstellen van nauwkeurige algoritmische profielen van gebruikers ertoe kan leiden dat individuen meer privacybeschermend gedrag gaan vertonen, wat toekomstige mogelijkheden voor gegevensverzameling kan beperken. Gebruikers ontwikkelen ook negatieve attitudes ten opzichte van het platform wanneer het advertenties toont die te gevoelige gegevens of meerdere soorten gegevens gebruiken. Aanbevolen wordt om selectiever te zijn in het verzamelen en gebruiken van gegevens, meer verantwoorde dataprakijken te hanteren en gebruikers betekenisvollere, zichtbare en gebruiksvriendelijke controlemogelijkheden te bieden.

Voor beleidsmakers en toezichthouders suggereren de bevindingen dat de huidige regelgeving mogelijk moet worden uitgebreid met een bredere lijst van bijzondere

categorieën van persoonsgegevens. De reden is dat veel datatypen die vaak voor adverteren worden gebruikt (bijv. locatie, zoekgeschiedenis) door consumenten als zeer gevoelig worden beschouwd, maar onder de huidige regelgeving nog niet als bijzondere categorie worden erkend of beschermd. Regelgeving zou ook volledige openheid moeten vereisen van alle gegevens die voor adverteren worden gebruikt, niet slechts de 'belangrijkste parameters', om geïnformeerde consumentenbeslissingen mogelijk te maken. Daarnaast wordt aanbevolen de reikwijdte van dataveillance verder te beperken en toegankelijke hulpmiddelen voor privacybescherming te waarborgen om privacy cynisme tegen te gaan en gebruikers in staat te stellen hun privacy te beschermen.

ALGEMENE CONCLUSIE

Alles bij elkaar genomen biedt dit proefschrift inzichten in de overtuigingen van individuen over dataveillance, de triggers en consequenties van perceived surveillance, en de individuele en contextuele factoren die hiermee samenhangen. Het concludeert dat surveillance door bedrijven een belangrijke drijvende kracht is achter percepties van surveillance bij individuen, en dat mensen zowel de voordelen als de kosten van surveillance zien. In situaties waarin mensen gegevensverzameling waarnemen, kunnen de gevoeligheid en hoeveelheid van gegevens en de nauwkeurigheid van voorspellingen die uit die gegevens worden gemaakt, de perceived surveillance versterken. Vervolgens gaan individuen met dit gevoel om door een verhoogde intentie om hun privacy te beschermen te tonen, maar mogelijk ook door privacy cynisme. Verder schaadt het gevoel gesurveilleerd te worden als gevolg van het zien van datagedreven advertenties, de attitudes van individuen ten opzichte van de advertentie, het merk en het platform. Tot slot varieert perceived surveillance ook met individuele verschillen en technologische contexten.


随着数字技术逐渐渗透到人们的日常生活中，越来越多的个人数据被收集、存储和处理，用于监管或管控个人及群体的行为，这种现象被称为“数据监控”（dataveillance）。在数字社会中，人们虽然难以追踪自身经历中的每一次数据收集行为，但其必然会在某些场景下意识到或是推测到自身数据正在被收集。这些经历会引发“感知监控”（perceived surveillance），即产生被监视、被监听，或是个人数据被记录的感受。本论文旨在探究公众对数据监控的认知，引发感知监控的因素，感知监控如何影响人们的应对方式（coping）与信息反应（message responses），以及哪些个体差异和技术场景与感知监控相关。进而理解这种被监控的感受。

论文研究目标

本论文设定了四项研究目标，这些目标旨在填补当前学界对感知监控理解中的四个关键研究空白。

一、梳理公众对数据监控的认知：

该目标聚焦于探究公众如何理解数据监控（包括他们认为谁在实施监控、监控的目的、监控的方式），以及他们对这些监控行为的评价（包括积极和消极的想法与感受）。

二、考察感知监控的具体触发因素：

该目标重点分析当公众发现自己的数据被收集时，究竟哪些因素会让他们产生被监控的感受。研究内容包括探究算法画像（algorithmic profiling）的“感知准确性”（perceived accuracy）与“客观准确性”(objective accuracy）所起的作用，以及用于数据驱动广告（data-driven advertising）的“数据敏感性”（sensitivity of data）与“数据量”(amount of data）对感知监控的影响。

三、研究感知监控对公众应对策略及公众对数据驱动广告态度的影响：

该目标围绕被监控感展开，分析其如何影响公众采取应对策略（如保护隐私的意愿、隐私犬儒主义），同时探究在数据监控用于数据驱动广告的场景下，这种被监控感如何影响公众对广告、品牌及平台的态度。

四、探索与感知监控相关的个体差异及场景因素：

该目标旨在研究感知监控的程度是否会因个体差异（如年龄、教育程度、对隐私的担忧程度不同）而不同，以及在多元技术场景（如社交媒体、智能设备）中，感知监控的程度是否有明显区别。

本论文通过四项实证研究展开分析。第一项研究（第二章）对 23 名荷兰成年人进行了深度访谈，重点了解他们对数据监控的民间理论（folk theories）、具体想法和感受。第二项研究（第三章）采用横断面调查（cross-sectional survey）方法，以 1994 名荷兰成年人为代表性样本，以定量的方法描述了人们感知到的监控来源与监控目的，并探究了与感知监控相关的个体差异及技术场景。第三项研究（第四章）同样采用横断面调查，邀请 685 名英国成年人查看自己在谷歌（Google）平台上的真实算法画像，分析算法画像的感知准确性与客观准确性如何与感知监控及不同应对策略相关联。第四项研究（第五章）以 1256 名英国成年人为研究对象开展线上实验，探究数据驱动广告中数据敏感性与数据量如何影响感知监控，以及这种影响对广告效果和“隐私犬儒主义”（privacy cynicism）产生的后果。

主要结论

综合本论文中的各项研究，最终得出六项关键结论：

关键结论一：数据驱动广告塑造了核心民间理论“企业为盈利不择手段收集数据”

本论文识别出公众关于数据监控的多种认知框架，这些认知基于感知到的监控来源（谁在监控）、监控目的（为什么监控）与监控机制（如何监控），共同构成了民间理论。其中最突出的民间理论是“企业为盈利不择手段收集数据”。这一认知主要源于公众对数据驱动广告的体验：荷兰群体的定量研究结果显示，广告商被视为数据监控的主要来源，而广告推广则被视为数据监控的主要目的。相较于政府监控或其他形式的监控，企业监控（尤其是以广告为目的的监控）在人们的日常数字体验中，被认为是更普遍存在的。公众的这种认知与“监控资本主义”（surveillance capitalism）的概念相符，说明人们能意识到企业以盈利为目标的本质。此外，公众认为技术虽是数据监控的直接来源，但最终仍受企业控制——这一发现为理解技术在数据监控中的作用提供了更细致的视角。

关键结论二：公众认为数据监控利弊共存

公众对数据监控的看法具有两面性。一方面，他们认可数据监控的好处，比如能改善用户体验、带来技术之外的益处（如健康水平提升），同时也普遍认可这些系统的智能性。另

一方面，人们觉得自己与数据收集方之间存在权力不对等，担心数据收集过程中存在不道德行为与隐私问题，会产生被侵犯感，并觉得这类行为令人不适。这一结论拓展了隐私计算模型（privacy calculus model），将被侵犯感、不适感等情感层面的因素纳入感知成本的范畴。

关键结论三：算法画像的准确性，以及数据驱动广告中所用数据的敏感性与数量均会影响感知监控

当公众观察到数据收集行为（如查看自己的算法画像、看到数据驱动广告）时，就会产生被监控感。而这些数据收集行为的具体特征，也会对感知监控产生影响。比如，当公众查看自己的算法画像时，算法画像的感知准确性与客观准确性都和感知监控呈正相关——画像越准确，人们越会觉得自己被监控。在数据驱动广告场景中，使用高敏感性数据（如收入、地理位置）或多种类型数据的广告，比使用低敏感性数据（如性别、年龄）或单一类型数据的广告，更容易引发强烈的被监控感。值得注意的是，无论数据量多少，使用高敏感性数据总能触发最强的感知监控，这说明数据的敏感性在触发感知监控的过程中起到了更关键的作用。该结论通过整合多种理论，解释了数据的具体特征或数据收集的结果如何导致不同程度的感知监控，同时提供了重要实证依据，丰富了相关领域的知识体系。

关键结论四：公众通过增强隐私保护意愿应对感知监控，但也可能滋生更强的隐私犬儒主义

面对日益强烈的被监控感，人们保护隐私的意愿通常会增强（比如通过调整广告设置）。另一种潜在应对策略是隐私犬儒主义，即认为保护隐私是徒劳的。不过，感知监控与隐私犬儒主义之间的关联并不稳定，这表明可能只有对个人影响较大的经历才能改变人们的隐私犬儒主义水平。此外，本论文还通过质性研究发现了其他对感知监控的应对策略，比如自我赋权（self-empowerment）、淡化数据监控的负面影响、对企业产生同情等。但这些应对策略与感知监控并无直接的正向关联，反而与算法画像的感知准确性直接相关，这说明可能还存在信任、意外感等其他作用机制。这些结论揭示并验证了公众应对数据监控的不同策略，有助于理解公众如何从认知层面在意识到数据监控与继续使用数字产品之间找到平衡。

关键结论五：感知监控会降低公众对广告、品牌及平台的好感

感知监控还会对公众如何看待广告产生负面影响。当人们因为看到数据驱动广告而产生被监控感时，不仅会对广告及背后品牌产生更负面的态度，还会对展示该广告的平台（如社

交媒体平台）产生负面态度。以往研究大多只关注公众对广告和品牌的评价，而本结论拓展了这一研究范围，揭示了当个人数据被用于说服性信息时，人们可能会对所有被认为参与数据监控的主体产生不满。同时，这一结论也挑战了“平台只是中立的信息渠道”这一观点，表明公众会要求平台对为数据驱动广告提供支持的数据监控行为负责。

关键结论六：感知监控的程度会因个体差异和技术场景不同而变化

感知监控与多项个体差异因素相关。首先，人们对隐私的担忧程度（privacy concerns）以及“阴谋论心态”（conspiracy mentality）越高，感知监控的程度越强；其次，年轻群体和高学历群体通常更容易觉得自己被监控；此外，“在线隐私素养”（online privacy literacy）会调节感知监控与隐私犬儒主义之间的关系。技术场景也会影响感知监控的程度：社交媒体和网页浏览器被认为是监控感最强的场景，而智能手表和智能家居设备则被认为是监控感最弱的场景。该结论用实证数据为“个体差异和场景因素会影响人们对数据监控的感受”这一观点提供了实证支持，有助于明确哪些人群更容易产生被监控感以及在哪些场景下人们更可能产生被监控感。

实践启示

本论文为广告主、广告平台及政策制定与监管机构提供了切实可行的建议。

对广告主而言，关键在于平衡广告个性化的益处与触发感知监控的弊端。建议谨慎选择用于个性化的数据源类型与数据量，尤其应避免使用高敏感性数据（如个人收入、实时位置、搜索记录、浏览记录、心理健康状况）或过量数据。遵循这些建议有助于降低公众的被监控感，减少其对广告、品牌及平台的负面评价。

对广告平台而言，为用户生成准确的算法画像可能会导致公众采取更多隐私保护行为，进而限制未来的数据收集可能性。此外，当平台推送的广告使用高敏感性数据或多类型数据时，用户也会对平台产生消极态度。建议平台需更审慎地选择数据收集与使用范围，采取更负责任的数据处理方式，并为用户提供更有意义、更可见且易于操作的隐私控制选项。

对政策制定与监管机构而言，研究结果表明当前法规可能需要扩展特殊类别数据（special category data）的涵盖范围。许多常用于广告的数据类型（如位置信息、搜索记录）被消费者视为高敏感性数据，但在现有法规中尚未被认定为特殊类别数据，也未得到相应保护。法规还应要求广告方全面披露用于广告的所有数据，而非仅披露主要参数，以帮助消费者

做出知情决策。此外，建议进一步限制数据监控的范围，并确保隐私保护工具的可及性，以应对隐私犬儒主义，增强用户的自主控制权。

总体结论

综上，本论文深入探究了公众对数据监控的认知、感知监控的触发因素与后果，以及与感知监控相关的个体和场景因素。研究结论如下：首先，企业监控是引发公众感知监控的主要因素。其次，公众认为数据监控利弊共存。在观察到数据收集行为的场景中，数据敏感性、数据量及基于数据所得推断的准确性，均会加剧感知监控强度。面对被监控感，公众会通过增强隐私保护意愿应对这种感受，但也可能滋生隐私犬儒主义。此外，因看到数据驱动广告而产生的被监控感，会损害公众对广告、品牌及平台的态度。最后，感知监控水平会因个体差异及技术场景的变化而有所不同。

AUTHOR CONTRIBUTIONS

Chapter 2: "They Know Everything": Folk Theories, Thoughts, and Feelings About Dataveillance in Media Technologies

Researchers: Dong Zhang (DZ), Sophie C. Boerman (SB), Hanneke Hendriks (HH), Margot J. van der Goot (MvdG), Theo Araujo (TA), Hilde Voorveld (HV)

Conceptualization: DZ, SB, HH, TA, HV

Methodology: DZ, SB, HH, MvdG, TA, HV

Data collection: DZ

Data analysis: DZ

Writing – original draft: DZ

Writing – review & editing: DZ, SB, HH, TA, HV

Funding acquisition: HV, TA, SB, HH

Chapter 3: A Peek Into Individuals' Perceptions of Surveillance

Researchers: Dong Zhang (DZ), Sophie C. Boerman (SB), Hanneke Hendriks (HH), Theo Araujo (TA), Hilde Voorveld (HV)

Conceptualization: DZ, SB, HH, TA, HV

Methodology: DZ, SB, HH, TA, HV

Data collection: DZ, TA

Data analysis: DZ

Writing – original draft: DZ

Writing – review & editing: DZ, SB, HH, TA, HV

Visualization: DZ

Funding acquisition: HV, TA, SB, HH

Chapter 4: Google Knows Me Too Well! Coping With Perceived Surveillance in an Algorithmic Profiling Context

Researchers: Dong Zhang (DZ), Joanna Strycharz (JS), Sophie C. Boerman (SB), Theo Araujo (TA), Hilde Voorveld (HV)

Conceptualization: DZ, JS, SB, TA, HV

Methodology: DZ, JS, SB, TA, HV

Data collection: DZ

Data analysis: DZ

Writing – original draft: DZ

Writing – review & editing: DZ, JS, SB, TA, HV

Visualization: DZ

Funding acquisition: HV, TA, SB, JS

Chapter 5: Too Sensitive, Too Much? Triggers and Consequences of Perceived Surveillance in Digital Data-Driven Advertising

Researchers: Dong Zhang (DZ), Joanna Strycharz (JS), Sophie C. Boerman (SB), Theo Araujo (TA), Hilde Voorveld (HV)

Conceptualization: DZ, JS, SB, TA, HV

Methodology: DZ, JS, SB, TA, HV

Data collection: DZ

Data analysis: DZ

Writing – original draft: DZ

Writing – review & editing: DZ, JS, SB, TA, HV

Visualization: DZ

Funding acquisition: HV, TA, SB, JS