



## UvA-DARE (Digital Academic Repository)

### Societal Consequences of Data-Driven Advertising

Strycharz, J.; Segijn, C.M.

**DOI**

[10.1007/978-3-031-86536-7\\_2](https://doi.org/10.1007/978-3-031-86536-7_2)

**Publication date**

2025

**Document Version**

Final published version

**Published in**

Rethinking Advertising

**License**

Article 25fa Dutch Copyright Act (<https://www.openaccess.nl/en/policies/open-access-in-dutch-copyright-law-taverne-amendment>)

[Link to publication](#)

**Citation for published version (APA):**

Strycharz, J., & Segijn, C. M. (2025). Societal Consequences of Data-Driven Advertising. In K. M. Vandenberg, & M. Tinger (Eds.), *Rethinking Advertising: Ethics and Effectiveness* (pp. 17-30). Palgrave Macmillan. [https://doi.org/10.1007/978-3-031-86536-7\\_2](https://doi.org/10.1007/978-3-031-86536-7_2)

**General rights**



It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.



# Societal Consequences of Data-Driven Advertising

*Joanna Strycharz*  and *Claire M. Segijn* 

## INTRODUCTION: SOCIETAL CONSEQUENCES OF DATA-DRIVEN ADVERTISING

Recent technological developments, such as advances in machine learning algorithms and artificial intelligence (AI), have greatly transformed the advertising landscape. Such technical possibilities paired with the low costs of collection and storage of consumer data as well as increased data processing capabilities through increasing hardware speeds have resulted in the emergence of so-called computational advertising (Huh and Malt-house 2020). Computational advertising can be defined as “a broad, data-driven advertising approach relying on or facilitated by enhanced

---

J. Strycharz (✉)

Amsterdam School of Communication Research, University of Amsterdam,  
Amsterdam, Netherlands

e-mail: [j.strycharz@uva.nl](mailto:j.strycharz@uva.nl)

C. M. Segijn

Hubbard School of Journalism & Mass Communication, University of  
Minnesota, Twin-Cities, USA

computing capabilities, mathematical models/algorithms, and the technology infrastructure to create and deliver messages and monitor/surveil an individual's behaviors" (Huh and Malthouse 2020, 1). This form of advertising depends on granular-level data collection, mining, aggregation, and ad serving, and is highly individualized (Helberger et al. 2020). Examples of such advertising include online behavioral advertising in which consumers' online behavior (e.g., likes, searches, and clicks) is tracked and subsequently used to show them individually targeted ads (Boerman et al. 2017), social media advertising in which one's social media profiles and other data collected about them are used to show them individually targeted ads on social networking sites (Knoll 2015), and online advertising that includes people's names (Bang and Wojdyski 2016) or relies on demographic targeting (Maslowska et al. 2011).

While consumers believe that such data-driven advertising is beneficial for them as they receive personally relevant messages and offers—which they experience as convenient (Strycharz et al. 2019)—it requires surveillance by advertisers who collect consumers' personal information such as their name and demographics, and monitor their behaviors such as online searches, location, and media consumption. This situation of automated, continuous, and unspecific collection of data by entities, such as advertisers, has been given the name of *dataveillance* (Büchi et al. 2022; Strycharz and Segijn 2022). It impacts individuals as it makes them feel watched and drives so-called surveillance responses, which encompass different responses that relate to being surveilled (Lyon 2017; Strycharz and Segijn 2022). Surveillance responses are a way for consumers to cope with their data being collected and involve cognitive (e.g., increased privacy concerns or resignation), affective (e.g., negative emotions related to dataveillance), and behavioral (e.g., taking additional privacy protection measures to prevent dataveillance) measures.

While dataveillance might trigger different responses among consumers, the centrality of consumer data can also change how consumers are affected by advertising. Data collection and processing gives advertisers the ability to translate consumer insights into targeted advertising strategies and decide who gets included in information, advertisements, and opportunities, and who does not (Bol et al. 2020). Furthermore, advertisers can use such insights to increase persuasiveness of online content by targeting individual characteristics or contexts and making advertising more personally relevant to the recipient (De Keyzer et al. 2022; Calo 2014). Dataveillance and computational advertising can

potentially lead to new disparities and exploitation of vulnerabilities of individual consumers (Helberger et al. 2022; Strycharz and Segijn 2022).

The extensive dataveillance paired with computational advertising and the possibilities such advertising opens to inform or persuade consumers raise several questions about the possible societal consequences. The current chapter takes the perspective of the society and individual consumers and focuses on the potential negative impact data-driven advertising has on them. First, we introduce the role of dataveillance in the current advertising landscape. Second, we focus on the (1) impact of dataveillance and (2) exploitation potential of computational advertising. The chapter concludes with a reflection on the potential of computational advertising that goes beyond persuasion.

## COMPUTATIONAL ADVERTISING AND THE ROLE OF DATAVEILLANCE

Computational advertising involves a data-driven advertising approach to creating and delivering personalized messages (Huh and Malthouse 2020). Consumers can be exposed to such advertising online (e.g., online behavioral advertising or social media advertising), offline (e.g., digital billboards), and across different media types (e.g., synced advertising) (Yun et al. 2020). One of the main catalyzers of the popularity of computational advertising has been the rising importance of the digital environment in consumers' daily lives and consequently, availability of consumer data and the possibility to analyze it with higher sophistication. Machine-learning and predictive-analytics models were developed to predict the likelihood of various customer actions and characteristics (Huh and Malthouse 2020). For example, Google, which relies heavily on computational advertising for its revenue, processes consumer data to place them into numerous categories that include demographics, life situation, interests, and needs (Google Ads API, 2024). For such categorization, availability of large amounts of consumer data is a prerequisite, which fosters the reality of dataveillance.

### *Dataveillance in the Advertising Landscape*

To add to our earlier definition of dataveillance, it describes the “automated, continuous, and (unspecific) collection, storage, and processing of digital traces from people or groups, by means of personal data systems

by state and corporate actors, to regulate or govern their behavior” (Strycharz and Segijn 2022, 576). It can be seen as a specific form of the broader phenomenon of surveillance that is characterized by the use of digital data (Kappeler et al. 2023). It should also be distinguished from simple data collection through its automation, large scale, and continuous character of the collection of digital traces (Strycharz and Segijn 2022).

Different actors can be a source of dataveillance, including companies and advertisers. In fact, due to developments in computational advertising, companies have become the main sources of (continuous) data collection in the digital society (Christl et al. 2017). For example, cookies—small text files put on users’ devices to either facilitate the functionality of a website (functional cookies) or collect information (tracking cookies)—have enabled companies to track website visits and follow the online behavior of individuals (Smit et al. 2014). More recently, new technology has increased possibilities to collect information about consumer behavior in the offline world. Smart devices such as smartphones or wearables are equipped with numerous sensors and connected to the Internet. This enables companies to collect new types of data (e.g., location data; physiological data), adding another dimension to the reach of dataveillance (Christl et al. 2017; Yun et al. 2020).

## IMPACT OF COMPUTATIONAL ADVERTISING ON CONSUMERS

The extensive dataveillance necessary for computational advertising might have negative effects both on society and on individual consumers. From the societal perspective, it contributes to the creation of so-called surveillance culture, a new notion that goes beyond the surveillance state commonly discussed in the twentieth century and related to governmental surveillance (Lyon 2017). Governmental surveillance is generally strongly linked to securitization, which reinforces the sense that surveillance is warranted and for the good of the individual and society (Lyon 2017). However, over time, corporations have started playing a central role in surveillance. In this context, the data is not used for security purposes, but to “predict and modify human behavior to produce revenue and market control” (Zuboff 2015, 75). While consumers could opt out from corporate surveillance in theory (e.g., reject cookies, opt out from advertising), in reality it might not be so easy because of a lack of transparency by companies and awareness by consumers regarding dataveillance (see

also Parfitt's comments about shadow text in Chapter 10 of this book), a lack of skills, a lack of motivation, or dependency on certain goods and services (Segijn et al. 2021; Lutz et al. 2020). In fact, surveillance is affecting many aspects of daily life. As a consequence, individuals, similar to all other actors in society, start playing an active role in such culture through changing their perceptions and behaviors (Lyon 2017). Along these lines, computational advertising that relies on dataveillance has the potential to elicit new types of responses, namely so-called surveillance responses (Strycharz and Segijn 2022).

### *Surveillance Responses to Computational Advertising*

Surveillance responses have been defined as responsive practices that relate to being surveilled (Lyon 2017). They can be triggered by different types of surveillance. For example, in the context of government surveillance, they might include installing encrypted protection from national security agencies or wearing clothing that limits camera recognition in public places (Lyon 2017). In the context of dataveillance for advertising, surveillance responses can be cognitive (i.e., cognitive coping), affective (i.e., emotional or attitudinal responses), and behavioral (i.e., actions).

Privacy cynicism has been recently introduced as a cognitive coping mechanism that allows consumers to overcome or ignore their concerns related to dataveillance and engage in online behaviors without ramping up privacy protection efforts (Hoffmann et al. 2016). It involves elements of mistrust, uncertainty, powerlessness, and resignation (Lutz et al. 2020), and it arises when people are faced with powerful and difficult to understand online services (Ranzini et al. 2023). In the reality of surveillance culture, consumers feel that they cannot avoid surveillance because there are few alternatives available that do not involve surveillance (Zhang et al. 2024). The dependency on services requiring personal data but offering consumers few alternatives creates an asymmetry in power (West 2019) and may result in the development of privacy cynicism among consumers (Lutz et al. 2020). Subsequently, privacy cynicism may weaken consumers' emancipatory privacy functions such as taking active control over how their data is collected or processed and making informed choices about it. As a result, consumers may be vulnerable to risk and exploitation, have lower trust in online institutions, and be excluded from economic opportunities (Ranzini et al. 2023).

Beyond cognitive coping, consumers might emotionally cope with dataveillance. Segijn and Van Ooijen (2020) investigated affective responses to data-driven advertising scenarios and concluded that consumers consider such ads creepy, annoying, and unsettling. Furthermore, data-driven advertising directly elicited negative affect such as dislike or hate, and consumers reported that such tactics make them upset or worried (Segijn and Van Ooijen 2020). When consumers see data-driven advertising as a threat, it could lead to affective reactance, which includes being more irritated, angry, annoyed, and aggravated (Farman et al. 2020). Additionally, awareness of data-driven advertising practices could lead to more critical attitudes and subsequent resistance toward such advertisements (Segijn et al. 2023).

Finally, consumers might turn to adjusting their behavior to cope with dataveillance (e.g., privacy protection, self-censorship) and its source (Lyon 2017). Past literature has distinguished between two main behavioral responses, namely (1) additional actions aimed at reducing dataveillance and (2) inhibitory practices (limiting disclosure) aimed at sidestepping dataveillance (Baruh et al. 2017). Additional actions involve adopting privacy protection measures and include installing ad blockers, employing cookie management, and using the private mode and Do Not Track functions in a browser (Boerman et al. 2018). Research by Boerman et al. (2018) has shown that experiencing data collection by companies as problematic is a driver of such protection behaviors.

Alternatively, consumers may respond with inhibitory practices and choose to self-censor the information they share online in case of voluntary online disclosure, or they may change their behavior to control what behavioral information can be collected about them—so-called chilling effects (Büchi et al. 2022). Chilling effects describe a situation in which consumers refrain from exhibiting certain behaviors to keep their data from being collected (Solove 2014). In the context of data-driven advertising, chilling effects can, for example, include not visiting websites that collect consumer data or not using smart devices that create the perception of surveillance (Penney 2021; Strycharz and Segijn 2022). From a societal perspective, the fact that dataveillance might lead to chilling effects among consumers is a serious ethical concern. Chilling effects can be seen as an extreme form of social conformity and are a threat to intellectual privacy as individuals limit their own access to information by choosing not to consume media freely, which forms a threat to their identity construction (Penney 2021) and autonomy (Büchi et al. 2022).

### *Manipulation Potential of Computational Advertising*

While the reliance of computational advertising on dataveillance leads to numerous societal and individual consequences, how the data can be used to personalize advertising raises concerns as well. Data-driven targeting strategies can be used to decide who is included in advertisements and information, and who gets excluded from them (Bol et al. 2020). For example, Bol et al. (2020) found that health-related sponsored content on Facebook was predominantly targeted at older users, females, and those with higher levels of trust in online companies, as well as those in poorer health conditions. Targeting specific audiences at the exclusion of others for access to information might result in biases and discrimination of individual consumers (Wachter and Mittelstadt 2024). Furthermore, such strategies can be applied to increase persuasiveness of online content by targeting individual characteristics that influence one's decision making (Calo 2014). In doing so, computational advertising leads not only to new opportunities but potentially also new disparities and exploitation of vulnerabilities in digital society, and in individuals (Bol et al. 2018).

Traditionally, in the context of advertising, certain groups of consumers have been considered vulnerable and hence in need of empowerment and greater protection. For example, adolescents are more impulsive and self-conscious than adults and hence more vulnerable to harm through manipulation (Pechmann et al. 2005). Along these lines, vulnerability has been commonly understood as a stable property or a characteristic of certain groups. In fact, the concept of traditional vulnerability singles out certain groups of consumers that are more susceptible to persuasion than others, and less able to protect themselves from unwanted influences (Helberger et al. 2022). Thus, this understanding singles out groups that are more susceptible to harm and manipulation than others, such as children (Livingstone and Third 2017).

Recently, it has been emphasized that the concept of vulnerability should not be used simply to describe designated groups of individuals, as belonging to such a group does not necessarily make them vulnerable, but vulnerability may fluctuate depending on the context or situation (Hill and Sharma 2020). Therefore, defining vulnerability based on group membership is limiting as it can be individual and contextual, i.e., stem from the situation one is in (Baker et al. 2005). In fact, vulnerability can stem from internal factors related to individual characteristics (e.g., literacy or biases) and states (e.g., motivation or stress), as well as external

factors, including lack of access to goods and services (e.g., having limited access to the internet) and the environment (e.g., the design of a website) (Strycharz and Duivenvoorde 2021). Instead of singling out groups, digital vulnerability describes “a universal state of defenselessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer–seller relations, and the very architecture of digital marketplaces” (Helberger et al. 2022, 176).

Regarding exploitation of digital vulnerabilities through computational advertising, as Calo (2014) argues, dataveillance and using the data to construct individual profiles “permits firms to surface the specific ways each individual consumer deviates from rational decision-making, however idiosyncratic, and leverage that bias to the firm’s advantage” (1003). Companies can use data to predict individual characteristics that may make them more vulnerable to persuasion and use these in their targeting strategy. For example, a computational advertisement can be specifically directed to a group of consumers who are likely to react to that advertisement less rationally due to a personality trait (psychographic segmentation, Graves and Matz 2018). Another potential issue arises when data is used to infer psychological states and specific life situations of individuals (Strycharz and Duivenvoorde 2021). Facebook allegedly offered advertisers the option to target young users in a state of psychological vulnerability, inferring when the users felt insecure and stressed (Tiku 2017). In a similar pattern, a marketing firm found that women felt less attractive on Mondays, especially in the morning, and recommended targeting women with beauty products specifically at that time of the week (PHD Media 2013). These examples demonstrate that computational advertising makes it possible to target consumers who are less rational due to their vulnerabilities, such as illness or psychological distress. Such advertising carries the danger of maintaining existing stereotypes and exploiting individual irrationalities (Strycharz and Duivenvoorde 2021).

## CONCLUSION: COMPUTATIONAL ADVERTISING BEYOND PERSUASION

Consumer data is central to today’s advertising tactics and strategies because it leads to more personalized and relevant advertising for the consumer (Yun et al. 2020). Besides benefits, such as convenience and financial gains (Strycharz et al. 2019), it also comes with its costs for

society and the consumer that go beyond persuasion. Such advertising is impactful for the society and individuals as it (1) requires extensive data collection and processing, (2) decides who is included in information, receives advertisements, and has access to opportunities, and who gets excluded, (3) allows companies to influence individuals' decision making by targeting their personal characteristics and contexts. Hence, it creates not only new opportunities, but also new challenges for and disparities in society and among individuals.

Data-driven advertising, such as computational advertising enabled by artificial intelligence and machine learning, may further contribute to data capitalism (West 2019) and surveillance culture (Lyon 2017). On a societal level, data-driven advertising can lead to biases, discrimination, and misinformation (Wachter and Mittelstadt 2024) as it may exclude consumers from information and create and exploit new vulnerabilities (Strycharz and Duivenvoorde 2021). On an individual level, it may affect consumers' autonomy (Segijn and Strycharz 2023) and affect their decision making (Helberger et al. 2022), especially when they are vulnerable.

Moving forward, we must consider how data can be used in an ethical way to limit the negative impacts on society and the individual. Transparency, accountability, and a positive impact on the economy and society have been suggested among the three key values in a society in which data and AI are central (Cath et al. 2017). Along these lines, in many jurisdictions, policymakers and regulators have recognized the need for new measures to address a range of emerging consumer risks in the digital world including surveillance and vulnerability exploitation (OECD 2024). For example, the recent regulatory frameworks (AI Act, the DMA, and the DSA) include a set of prohibitions on problematic digital market actors' behavior that might exploit individual consumers (Morozovaite 2022). The extent of, and infrastructure for, data collection and processing for data-driven advertising resulting in a situation of dataveillance open new questions regarding the impact of advertising. Thus, further research is required to minimize risks and ensure positive value of advertising for the society and individuals.

**Competing Interests** The authors have no conflicts of interest to declare that are relevant to the content of this chapter.

## REFERENCES

- Baker, Stacey Menzel, James W. Gentry, and Terri L. Rittenburg. 2005. "Building Understanding of the Domain of Consumer Vulnerability." *Journal of Macromarketing* 25 (2): 128–39. <https://doi.org/10.1177/0276146705280622>.
- Bang, Hyejin, and Bartosz W. Wojdyski. 2016. "Tracking Users' Visual Attention and Responses to Personalized Advertising Based on Task Cognitive Demand." *Computers in Human Behavior* 55 (February): 867–76. <https://doi.org/10.1016/j.chb.2015.10.025>.
- 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>.
- Boerman, Sophie C., Sanne Kruikemeier, and Frederik J. Zuiderveen Borge-sius. 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, Sophie C., Sanne Kruikemeier, and Frederik J. Zuiderveen Borge-sius. 2018. "Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data." *Communication Research* 48 (7). <https://doi.org/10.1177/0093650218800915>.
- Bol, Nadine, Joanna Strycharz, Natali Helberger, Bob van de Velde, and Claes H de Vreese. 2020. "Vulnerability in a Tracked Society: Combining Tracking and Survey Data to Understand Who Gets Targeted with What Content." *New Media & Society* 22 (11): 1996–2017. <https://doi.org/10.1177/1461444820924631>.
- Bol, Nadine, Natali Helberger, and Julia C. M. Weert. 2018. "Differences in Mobile Health App Use: A Source of New Digital Inequalities?" *The Information Society* 34 (3): 183–93. <https://doi.org/10.1080/01972243.2018.1438550>.
- 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): 205395172110653. <https://doi.org/10.1177/20539517211065368>.
- Calo, M. Ryan. 2014. "Digital Market Manipulation." *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2309703>.
- Cath, Corinne, Sandra Wachter, Brent Mittelstadt, Mariarosaria Taddeo, and Luciano Floridi. 2017. "Artificial Intelligence and The 'Good Society': The US, EU, and UK Approach." *Science and Engineering Ethics* 24 (1). <https://doi.org/10.1007/s11948-017-9901-7>.
- Christl, Wolfie, Katharina Kopp, and Patrick Urs Riechert. 2017. "Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze,

- Trade, and Use Personal Data on Billions.” Cracked Labs. Cracked Labs. 2017. <https://crackedlabs.org/en/corporate-surveillance>.
- De Keyzer, Freya, Nathalie Dens, and Patrick De Pelsmacker. 2022. “Let’s Get Personal: Which Elements Elicit Perceived Personalization in Social Media Advertising?” *Electronic Commerce Research and Applications* 55 (September): 101183. <https://doi.org/10.1016/j.elerap.2022.101183>.
- Farman, Lisa, Maria Leonora (Nori) Comello, and Jeffrey R. Edwards. 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>.
- Google Ads API. 2024. “Codes and Formats.” Google for Developers. 2024. <https://developers.google.com/google-ads/api/data/codes-formats>.
- Graves, Christopher, and Sandra Matz. 2018. “What marketers should know about personality-based marketing.” *Harvard Business Review*. Retrieved from: <https://hbr.org/2018/05/what-marketers-should-know-about-personality-based-marketing>
- Helberger, Natali, Jisu Huh, George Milne, Joanna Strycharz, and Hari Sundaram. 2020. “Macro and Exogenous Factors in Computational Advertising: Key Issues and New Research Directions.” *Journal of Advertising* 49 (4): 377–93. <https://doi.org/10.1080/00913367.2020.1811179>.
- Helberger, Natali, M. Sax, J. Strycharz, and H. W. Micklitz. 2022. “Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability.” *Journal of Consumer Policy* 45: 175–200. <https://doi.org/10.1007/s10603-021-09500-5>.
- Hill, Ronald Paul, and Eesha Sharma. 2020. “Consumer Vulnerability.” *Journal of Consumer Psychology* 30 (3). <https://doi.org/10.1002/jcpy.1161>.
- 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>.
- Huh, Jisu, and Edward C. Malhouse. 2020. “Advancing Computational Advertising: Conceptualization of the Field and Future Directions.” *Journal of Advertising* 49 (4): 367–76. <https://doi.org/10.1080/00913367.2020.1795759>.
- Kappeler, Kiran, Noemi Festic, and Michael Latzer. 2023. “Dataveillance Imaginaries and Their Role in Chilling Effects Online.” *International Journal of Human-Computer Studies* 179 (November): 103120. <https://doi.org/10.1016/j.ijhcs.2023.103120>.
- Knoll, Johannes. 2015. “Advertising in Social Media: A Review of Empirical Evidence.” *International Journal of Advertising* 35 (2): 266–300. <https://doi.org/10.1080/02650487.2015.1021898>.

- Livingstone, Sonia, and Amanda Third. 2017. "Children and Young People's Rights in the Digital Age: An Emerging Agenda." *New Media & Society* 19 (5): 657–70. <https://doi.org/10.1177/1461444816686318>.
- 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>.
- Lyon, David. 2017. "Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity." *International Journal of Communication* 11: 19. <https://docslib.org/doc/10701384/surveillance-culture-engagement-exposure-and-ethics-in-digital-modernity>
- Maslowska, Ewa, Bas van den Putte, and Edith G. Smit. 2011. "The Effectiveness of Personalized E-Mail Newsletters and the Role of Personal Characteristics." *Cyberpsychology, Behavior, and Social Networking* 14 (12): 765–70. <https://doi.org/10.1089/cyber.2011.0050>.
- Morozovaite, Viktorija. 2022. "Hypernudging in the Changing European Regulatory Landscape for Digital Markets." *Policy & Internet*, October. <https://doi.org/10.1002/poi3.329>.
- OECD. 2024. "Consumer Vulnerability in the Digital Age." OECD. 2024. [https://www.oecd.org/en/publications/consumer-vulnerability-in-the-digital-age\\_4d013cc5-en.html](https://www.oecd.org/en/publications/consumer-vulnerability-in-the-digital-age_4d013cc5-en.html).
- Pechmann, Cornelia, Linda Levine, Sandra Loughlin, and Frances Leslie. 2005. "Impulsive and Self-Conscious: Adolescents' Vulnerability to Advertising and Promotion." *Journal of Public Policy & Marketing* 24 (2): 202–21. <https://doi.org/10.1509/jppm.2005.24.2.202>.
- Penney, Jon. 2021. "Understanding Chilling Effects." *Papers.ssrn.com*. Rochester, NY. 28 May, 2021. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3855619](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855619).
- PHD Media. 2013. "New Beauty Study Reveals Days, Times and Occasions When U.S. Women Feel Least Attractive." <https://www.prnewswire.com/news-releases/new-beauty-study-reveals-days-times-and-occasions-when-us-women-feel-least-attractive-226131921.html>.
- Ranzini, Giulia, Christoph Lutz, and Christian Pieter Hoffmann. 2023. "Privacy Cynicism." *Routledge EBooks*, April, 134–143. <https://doi.org/10.4324/9781003244677-15>.
- Segijn, Claire M., and Iris Van Ooijen. 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, Claire M., and Joanna Strycharz. 2023. "The Ethical Ramifications of Surveillance in Contemporary Advertising for the Industry, Consumers,

- and Regulators: Current Issues and a Future Research Agenda.” *International Journal of Advertising*, 1–9, September. <https://doi.org/10.1080/02650487.2022.2114700>.
- 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): 317–338. <https://doi.org/10.1080/13527266.2021.2020149>.
- Segijn, Claire, Joanna Strycharz, Amy Riegelman, and Cody Hennesy. 2021. “A Literature Review of Personalization Transparency and Control: Introducing the Transparency-Awareness-Control Framework.” *Media and Communication* 9(4). <https://doi.org/10.17645/mac.v9i4.4054>.
- Smit, Edith G., Guda Van Noort, and Hilde A.M. Voorveld. 2014. “Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe.” *Computers in Human Behavior* 32 (March): 15–22. <https://doi.org/10.1016/j.chb.2013.11.008>.
- Solove, Daniel J. 2014. “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *Ssrn.com*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=998565](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565).
- Strycharz, Joanna, and Bram Duivenvoorde. 2021. “The Exploitation of Vulnerability through Personalised Marketing Communication: Are Consumers Protected?” *Internet Policy Review* 10 (4). <https://doi.org/10.14763/2021.4.1585>.
- 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>.
- Strycharz, Joanna, Guda van Noort, Edith Smit, and Natali Helberger. 2019. “Consumer View on Personalized Advertising: Overview of Self-Reported Benefits and Concerns.” *European Advertising Academy*, 53–66. [https://doi.org/10.1007/978-3-658-24878-9\\_5](https://doi.org/10.1007/978-3-658-24878-9_5).
- Tiku, Nitasha. 2017. “Welcome to the Next Phase of the Facebook Backlash.” *Wired*. May 21, 2017. <https://www.wired.com/2017/05/welcome-next-phase-facebook-backlash/>.
- Wachter, Sandra, and Brent Mittelstadt. 2024. “No Need to Wait for the Future: The Danger of AI Is Already Here.” *Ox.ac.uk*. <https://www.oii.ox.ac.uk/news-events/news/no-need-to-wait-for-the-future-the-danger-of-ai-is-already-here/>.
- West, Sarah Myers. 2019. “Data Capitalism: Redefining The Logics Of Surveillance And Privacy.” *Business & Society*, 58 (1): 20–41. <https://doi.org/10.1177/0007650317718185>
- Yun, Joseph T., Claire M. Segijn, Stewart Pearson, Edward C. Malthouse, Joseph A. Konstan, and Venkatesh Shankar. 2020. “Challenges and Future Directions

- of Computational Advertising Measurement Systems.” *Journal of Advertising* 49 (4): 1–13. <https://doi.org/10.1080/00913367.2020.1795757>.
- Zhang, Dong, Sophie C. Boerman, Hanneke Hendriks, van, Theo Araujo, and Hilde Voorveld. 2024. “‘They Know Everything’: Folk Theories, Thoughts, and Feelings about Dataveillance in Media Technologies.” *International Journal of Communication* 18. <https://hdl.handle.net/11245.1/c8c3c1ba-30ba-407c-a122-35384807c0cc>.
- Zuboff, Shoshana. 2015. “Big Other: Surveillance Capitalism And The Prospects Of An Information Civilization.” *Journal of Information Technology*, 30 (1): 75-89. <https://doi.org/10.1057/jit.2015.5>