PRIVACY-ENHANCING TECHNOLOGIES IN ADTECH AND CONSUMERS' PERCEIVED PRIVACY VIOLATIONS

BY KINSHUK JERATH

& LORENZO MICHELOZZI

Kinshuk Jerath is the Arthur F. Burns Chair of Free and Competitive Enterprise, Professor of Business in the Marketing Division at the Graduate School of Business, Columbia University. Lorenzo Michelozzi is a Principal at Cornerstone Research. The views expressed herein are those of the authors and do not necessarily represent the views of Cornerstone Research. This article is based in part on academic work that Kinshuk Jerath conducted together with Klaus Miller. Klaus Miller is an Assistant Professor in the Marketing Department at HEC Paris and a Chairholder at the Hi!Paris Center on Data Analytics and Artificial Intelligence for Science, Business and Society. The authors thank Coby Wittman for his outstanding assistance with the preparation of this article. Coby Wittman is an Associate at Cornerstone Research.

Visit www.competitionpolicyinternational.com for access to these articles and more!

PRIVACY-ENHANCING TECHNOLOGIES IN ADTECH AND CONSUMERS' PERCEIVED PRIVACY VIOLATIONS

By Kinshuk Jerath & Lorenzo Michelozzi

In response to growing consumer privacy concerns and governmental regulations, privacy-enhancing technologies ("PETs") are being developed in the AdTech space to allow ad targeting while limiting the flow and use of user data relative to current practices. Will PETs succeed in alleviating consumers' privacy concerns? A recent study by Professors Kinshuk Jerath and Klaus Miller suggests that PETs can reduce consumers' perceived privacy violations relative to current practices. The reduction, however, is small. Other practices that do not allow the targeting of online ads based on consumer behavior, such as contextual advertising, achieve more substantial reductions. These findings suggest that consumers' perceived privacy violations are affected less by technical details of whether/how the data is shared and more by expectations on how it is used and how individual-specific the outcomes will be. A consumer-centric approach to developing privacy solutions in AdTech, which more holistically considers consumers' perceived privacy violations, is recommended. Consumer education on privacy-enhancing initiatives may also help to bridge the gap between technical definitions of privacy and consumers' perceptions.

01
INTRODUCTION

Growing privacy concerns among consumers over the use of their data for online advertising have spurred the development and implementation of *privacy-enhancing technologies* ("PETs").[2] PETs are intended to allow advertisers to target relevant audiences online while limiting the flow and use of consumer data that is required to do so. While the technical aspects of PETs have received considerable attention, little is known about how consumers may receive them. Will PETs succeed in alleviating privacy concerns about the collection and use of consumer data for targeted advertising?

A recent study by Professors Kinshuk Jerath and Klaus Miller sheds light on this question. The authors use an online experiment to examine consumers' perceptions of privacy violations for current advertising practices as well as for practices akin to certain prominent PETs being implemented or developed. These PETs allow firms to target ads to individual users based on data that does not leave consumers' devices and is therefore not shared with third parties. The authors find that, relative to current practices, these PETs can reduce consumers' perceived privacy violations. The reduction, however, is small. Other practices that do not target advertising based on consumer characteristics or browsing histories, such as contextual advertising, reduce consumers' perceived privacy violations more substantially. The experimental results of Jerath and Miller suggest that consumers' perceived privacy violations are affected less by whether/how the data is shared (does it leave the device?) and more by expectations on how it is used and how individual-specific ads can get (is the data used to target ads effectively based on behavior?).

This article first provides an introduction to PETs and discusses some prominent examples being developed as part of Google's Privacy Sandbox. It then presents the findings of the Jerath and Miller study and discusses their interpretation. The article concludes by elaborating on the implications of the findings. Firms and policy-makers may want to adopt a consumer-centric approach to PETs that more holistically considers consumers' perceived privacy violations and also addresses the tradeoff that consumers face in practice between the perceived privacy costs of sharing data and the benefits that arise from the provision of advertising-funded content and services online. Consumer education on privacy-enhancing initiatives may also help to bridge the gap between technical definitions of privacy and consumers' perceptions.

02
THE EMERGENCE OF PRIVACY-ENHANCING TECHNOLOGIES IN RESPONSE TO PRIVACY CONCERNS

Behavioral targeting has become the online advertising industry's standard for display advertising. Under behavioral targeting, information about a consumer's activity is tracked over time and across websites and used to build user-level profiles attempting to understand the consumer's demographic characteristics (e.g. gender, age group, location) and interests (e.g. travel, fitness, sport). Consumers' characteristics and interests can then be used to target the ads that consumers encounter as they consume online content and services. Targeted ads have been shown to be more effective than untargeted ones,[3] suggesting that targeting improves the relevance of these ads to consumers. And to this day, online advertising remains the main source of revenue for many websites and publishers, allowing them to offer high-quality and free content and services to consumers.[4]

While targeted ads support online content and services that consumers enjoy, behavioral targeting elicits privacy con-

2 PETs can broadly be defined as technologies that "permit the collection, processing, analysis, and sharing of information, while protecting the confidentiality of personal data." See *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, OECD Digital Economy Papers (March 8, 2023), https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm.

3 See, e.g. Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, Management Science 57(1), 57-71 (2011); Paul R. Hoban & Randolph E. Bucklin, *Effects of Internet Display Advertising in the Purchase Funnel: Model-Based Insights from a Randomized Field Experiment*, Journal of Marketing Research 52(3), 375-393 (2015); Nils Wernerfelt, Anna Tuchman, Bradley Shapiro & Robert Moakler, *Estimating the Value of Offsite Tracking Data to Advertisers: Evidence from Meta*, forthcoming in Marketing Science.

4 Benjamin Shiller, Joel Waldfogel & Johnny Ryan, *The Effect of Ad Blocking on Website Traffic and Quality*, The RAND Journal of Economics 49(1), 43-63 (2018).

cerns.[5] In response to these and other similar concerns, privacy regulation has become more stringent with the introduction of laws, such as the General Data Protection Regulation ("GDPR") in the European Union or the California Consumer Privacy Act ("CCPA"), which seek to give users more control over their data and require firms to give users the right to opt-out from sharing their personal information. Recognizing consumer apprehension to data sharing, in the last few years, private companies have also launched initiatives to limit data collection and behavioral tracking and give consumers more control over their data. For example, in 2021, Apple adopted App Tracking Transparency, a framework that requires iOS apps to request permission from users before tracking their activity across other companies' apps or websites or sharing data with data brokers.[6] Web browsers such as Firefox and Safari have taken measures to stop third parties from tracking users' activity across websites by disabling third-party cookies as part of their standard settings.[7]

Against this backdrop, firms have also begun implementing or developing PETs to maintain the efficacy of advertising while addressing privacy concerns. Some of the most prominent examples of PETs are being developed under Google's Privacy Sandbox, an initiative that aims to reduce cross-site tracking while allowing publishers and developers to serve relevant content and ads.[8] Within the Sandbox toolkit, Google proposed two technologies that would directly impact how behavioral data used to target online ads is collected, processed, and shared: "Topics" and "Protected Audience."[9]

The "Topics" technology allows web browsers to infer interest-based categories associated with the websites a consumer visits. For example, the browser would match a sports website with the topic "Sports." This matching process occurs on the consumer's device without sharing information about the specific website visited with third parties, as it is currently done, for example, by third-party cookies. The most frequent topics associated with the websites visited by the consumer would then be shared with advertisers to help them show ads relevant to these topics on the websites the consumer visits.[10]

"Against this backdrop, firms have also begun implementing or developing PETs to maintain the efficacy of advertising while addressing privacy concerns"

The "Protected Audience" technology uses a consumer's activity to assign them to audiences that advertisers have defined for ad targeting purposes. For example, a bike maker may have defined an audience of "mountain bike enthusiasts" for consumers that have browsed mountain bikes on its website.[11] The "Protected Audience" technology allows the bike maker to show ads about mountain bikes to members of this audience when they visit a different website, say a sports magazine's site. Unlike current practices, the process that leads to the display of the bike maker's ad on the sports magazine's webpage occurs

5 For example, according to a 2019 Pew Research survey, 79 percent of Americans were concerned about how their data is collected and used by companies. This figure rose to 81 percent in a similar survey conducted in 2023. Additionally, according to the 2019 survey, 81 percent of Americans thought the risks of data collection outweigh the benefits. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/; Colleen McClain et al., *How Americans View Data Privacy*, Pew Research Center (October 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

6 Kinshuk Jerath, *Mobile Advertising and the Impact of Apple's App Tracking Transparency Policy* (April 26, 2022), https://www.apple.com/privacy/docs/Mobile_Advertising_and_the_Impact_of_Apples_App_Tracking_Transparency_Policy_April_2022.pdf.

7 Marissa Wood, *Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default*, Firefox (September 3, 2019), https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/; Nick Statt, *Apple Updates Safari's Anti-Tracking Tech with Full Third-Party Cookie Blocking*, The Verge (March 24, 2020), https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking; John Wilander, *Full Third-Party Cookie Blocking and More*, WebKit (March 24, 2020), https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/.

8 Google, as well, had seriously considered disabling third-party cookies from the Chrome browser. However, it recently decided to keep them as it continues to develop its Privacy Sandbox initiatives. See *Protecting Your Privacy Online*, Google Privacy Sandbox, https://privacysandbox.com/; *Prepare for the third-party cookie phaseout*, Google Privacy Sandbox (March 13, 2024), https://developers.google.com/privacy-sandbox/3pcd/prepare/prepare-for-phaseout; Anthony Chavez, *A New Path for Privacy Sandbox on the Web*, The Privacy Sandbox (July 22, 2024), https://privacysandbox.com/news/privacy-sandbox-update/.

9 *Technology for a more private internet*, Google Privacy Sandbox, https://privacysandbox.com/learning-hub/.

10 *Topics*, The Privacy Sandbox, https://privacysandbox.com/proposals/topics/.

11 *Protected Audience API overview*, Privacy Sandbox (January 27, 2022), https://developers.google.com/privacy-sandbox/relevance/protected-audience.

on the consumer's device.[12] Thus, while "Protected Audience" allows for more fine-grained targeting than "Topics," a key common feature of both these targeting technologies is that they keep the consumer's information on the consumer's device without sharing their browsing histories with third parties.

While PETs ultimately aim to benefit consumers by improving privacy protections, little is known about consumers' perceptions of PETs' ability to address privacy concerns. In fact, a lot of the discussion about PETs has been devoted to technical aspects and details related to data collection and usage by firms that PETs permit.[13] However, because digital advertising relies on consumer-facing technologies, it is important to understand whether and how these technologies can successfully address consumers' needs and wants.[14] Understanding consumers' perceptions is also important for policy-makers if their goal is to ensure that privacy regulations adequately address consumers' concerns.

03

NEW EVIDENCE ON CONSUMER PERCEPTIONS OF PRIVACY VIOLATIONS

In order to evaluate privacy violations that consumers may perceive in relation to behavioral tracking and PETs, it is important to understand the two types of value consumers place on privacy. The first is the intrinsic value of privacy, which refers to the disutility consumers may experience when their information is shared, regardless of how their information is used (even if not used at all). The second is the instrumental value of privacy, which refers to the disutility consumers experience if they dislike how their information is used (e.g. internet browsing information may allow firms to price discriminate, leading certain consumers to be charged higher prices). Instrumental value can also refer to the positive utility that consumers experience if, instead, they like how the information is used (e.g. video-content recommendations based on viewing history). While PETs may work to address the intrinsic value of privacy (e.g. by stopping consumer data from leaving their local device), they may not address the instrumental value if consumers find that companies can effectively use their data for profiling and targeting even if it was processed locally.

A recent study by Professors Kinshuk Jerath and Klaus Miller provides experimental evidence about consumers' perceptions of privacy violations through the lens of the dual privacy framework.[15] In their study, the authors present experimental subjects with different scenarios regarding data sharing and targeted advertising and ask them to rate the extent to which they perceive their privacy to be violated.

The authors consider a spectrum of scenarios that vary the level of intrinsic and instrumental values consumers are likely to experience, ranging from a behavioral targeting scenario (akin to the current practice in which consumers are targeted at the individual level and data leaves their devices), to a contextual targeting scenario (in which ads are targeted based on the content of the website the con-

12 When a consumer visits the sports magazine webpage, an auction is run to determine what ad to show to the consumer. Membership in the "mountain bike enthusiasts" audience can be one of the parameters used in the auction to select the most relevant ad. The main difference from current practice is that information about audience membership is stored on the consumer's device and the auction itself, as well, is run on the device. See *Protected Audience API overview*, Privacy Sandbox (January 27, 2022), https://developers.google.com/privacy-sandbox/relevance/protected-audience.

13 Recent academic research on PETs has examined their implication for research, studied their potential impact on advertisers and publishers, and documented the adoption of Privacy Sandbox technologies over time, but has not investigated consumers' perceptions. Policy discussions of PETs have also not examined consumers' perceptions. For example, in a report on PETs, the OECD discussed the potential of PETs to give consumers more control and protection over their data but did not address consumers' perceptions or expectations regarding PETs. Similarly, in a recent request for information, the U.S. Office of Science and Technology Policy stated that PETs present "a key opportunity to harness the power of data and data analysis techniques in a secure, privacy-protecting manner," but did not mention how consumers may respond to or perceive them. The FTC also recently highlighted the possibility for firms to make false or misleading representations regarding PETs but made no reference to consumers' attitudes. See Garrett A. Johnson, Julian Runge & Eric B. Seufert, *Privacy-Centric Digital Advertising: Implications for Research,* Customer Needs and Solutions 9(1), 49–54 (2022); Miguel Alcobendas, Shunto Kobayashi, Ke Shi & Matthew Shum, *The Impact of Privacy Protection on Online Advertising Markets* (Working Paper, 2023); Garrett A. Johnson & Nico Neumann, *The Advent of Privacy-Centric Digital Advertising: Tracing Privacy-Enhancing Technology Adoption*, (Manuscript, March 21, 2024); *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, OECD Digital Economy Papers (March 8, 2023); *Request for Information on Advancing Privacy-Enhancing Technologies*, Science and Technology Policy Office (June 9, 2022); *Keeping Your Privacy Enhancing Technology (PET) Promises*, Federal Trade Commission (February 1, 2024).

14 Standard marketing practice suggests that firms must understand how consumers "think, feel, and act." See Philip Kotler & Kevin Keller, *Marketing Management*, 15th Edition, Pearson (2016), p. 179.

15 Kinshuk Jerath & Klaus Miller, *Consumers' Perceived Privacy Violations in Online Advertising* (Working Paper, 2024).

sumer visits and nothing else), and a hypothetical scenario with no advertising and no targeting. Within this spectrum, the authors also consider two scenarios related to PETs, in which consumers' data does not leave their devices. In the first, consumers are targeted with ads at a group level based on interests (akin to Google's "Topics" technology discussed above), and in the second, they are targeted at the individual level (akin to Google's "Protected Audience" technology discussed above).

The authors find that consumers exhibit a small decrease in their perceived privacy violations under the PETs scenarios compared to the behavioral targeting scenario. More substantial declines in perceived privacy violations are observed for the contextual targeting scenario, both relative to the behavioral targeting scenario and the two PET scenarios. Additionally, the authors find that consumers only mildly prefer no ads to contextually targeted ads.

These findings suggest that privacy perceptions about user tracking and online advertising are affected less by the control users are given over whether/how the data is shared (does it leave the device?), and more by the expectations on how the data is used (is the data used to target ads effectively based on behavior?). This implies that while PETs may address concerns related to the intrinsic value of privacy, they may not fully address concerns pertaining to the instrumental value of privacy, and the latter may be large in magnitude.

In interpreting Jerath's and Miller's experimental findings, it is important to note that, in practice, consumers face a tradeoff between maintaining their information private and obtaining instrumental benefits from sharing that information. While Jerath's and Miller's study focuses on consumers' perceptions, these may be different from what might be inferred from revealed preference studies, i.e. analyses of consumer choices in the real world. For instance, it is well known that consumers say that they value privacy highly but then give up their data relatively easily in exchange for a small benefit.[16] This fact, known as the "privacy paradox," may then be resolved by recognizing that instrumental benefits of data sharing may actually outweigh the intrinsic disutility and instrumental costs associated with it.[17] In other words, while consumers may perceive their privacy to be violated when surveyed, in practice, they may perceive the instrumental benefits they receive sufficient to justify sharing their information.

In the case of behavioral advertising (or other types of well-targeted advertising), these instrumental benefits include: (i) seeing advertisements for more relevant products and (ii) being able to access free content and services on websites or applications funded by advertising revenue. Academic research shows that ads produce higher revenue and better consumer responses when they can rely on third-party cookies that track users across sites. For example, Goldfarb and Tucker (2011) found that privacy laws that limited targeted advertising reduced user purchase intent by 65 percent.[18] More recent research has found that publisher revenue would substantially decrease if third-party cookies were banned. For example, Alcobendas et al. (2021) find that publisher revenue would decline by 54 percent,[19] and a 2019 study by Google found that publisher revenue would decline by 52 percent.[20] Lower revenue may reflect a reduced salience of the ads for consumers. In turn, lower revenue may adversely affect the quality and quantity of free content that publishers and app developers make available to consumers online.[21]

16 Patricia Norberg, Daniel Horne & David Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, Journal of Consumer Affairs 4(1), 100-126 (2007); Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk* (NBER, Working Paper No. 23488, 2017).

17 For example, a recent study finds a positive relationship between consumers' preference for privacy and the amount of information sharing they engage in. This finding suggests that even for the most privacy-sensitive consumers, the instrumental benefits of sharing information may outweigh the intrinsic and instrumental costs. See Long Chen, Yadong Huang, Shumiao Ouyang & Wei Xiong, *Data Privacy and Digital Demand* (Working Paper, 2024).

18 Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, Management Science 57(1), 57-71 (2011).

19 Miguel Alcobendas, Shunto Kobayashi, Ke Shi & Matthew Shum, *The Impact of Privacy Protection on Online Advertising Markets* (Working Paper, 2023).

20 Relatedly, the UK CMA replicated Google's results in a report published in 2020 using only UK users and found a decrease in publisher revenue as high as 70 percent. Deepak Ravichandran & Nitish Korula, *Effect of Disabling Third-Party Cookies on Publisher Revenue*, Google, 2019; Competition and Markets Authority, *Online Platforms and Digital Advertising: Market Study Final Report*, 2020.

21 Benjamin Shiller, Joel Waldfogel & Johnny Ryan, *The Effect of Ad Blocking on Website Traffic and Quality*, The RAND Journal of Economics 49(1), 43-63 (2018); Tobias Kircher & Jens Foerderer, *Ban Targeted Advertising? An Empirical Investigation of the Consequences for App Development*, Management Science 70(2), 1070–1092 (2023); Garrett A. Johnson, Tesary Lin, James C. Cooper & Liang Zhong, *COPPAcalypse? The YouTube Settlement's Impact on Kids Content* (Working Paper, 2024).

04
CONCLUSION

The findings of Jerath and Miller indicate that, as far as privacy perceptions are concerned, consumers care more about the outcome of targeted advertising rather than the process of how it comes about. This suggests that it may be helpful for firms to adopt a more consumer-centric approach that addresses concerns over how information is used rather than rely solely on the technical particulars of how information is processed. Further, realizing that, in practice, consumers face a tradeoff between keeping information private and obtaining instrumental benefits of sharing that information, firms may also want to take measures to educate consumers on privacy-enhancing technologies and initiatives being developed. In addition, firms may want to take steps to directly address consumers' perceptions about both the process of online advertising as well as its outcomes. Consumer education on privacy-enhancing initiatives may thus be useful in bridging the gap between technical definitions of privacy and consumers' perceptions.

Current regulatory initiatives focus primarily on the intrinsic aspects of privacy (control, collection, and data security). The findings of Jerath and Miller show that instrumental aspects of privacy (how the data are used for targeting, such as making inferences from it) also deserve importance in designing policy. Directions from policy-makers may prompt developers of future PETs to address instrumental concerns about privacy that current proposals do not seem to alleviate. ■

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL