Privacy and Consumer Empowerment in Online Advertising

Other titles in Foundations and Trends® in Marketing

Aggregate Advertising Expenditure in the U.S. Economy: Measurement and Growth Issues in the Digital Era
Alvin J. Silk and Ernst R. Berndt
ISBN: 978-1-68083-872-5

Brands: An Integrated Marketing, Finance, and Societal Perspective
Bobby J. Calder
ISBN: 978-1-68083-746-9

Machine Learning in Marketing: Overview, Learning Strategies, Applications, and Future Developments
Vinicius Andrade Brei
ISBN: 978-1-68083-720-9

Crowdfunding Platforms: Ecosystem and Evolution
Yee Heng Tan and Srinivas K. Reddy
ISBN: 978-1-68083-698-1

A Practical Approach to Sales Compensation: What Do We Know Now? What Should We Know in the Future?
Doug J. Chung, Byungyeon Kim and Niladri B. Syam
ISBN: 978-1-68083-684-4

Privacy and Consumer Empowerment in Online Advertising

W. Jason Choi
Assistant Professor of Marketing
Rutgers Business School
USA
jason.choi@rutgers.edu

Kinshuk Jerath
Professor of Business
Marketing Division
Columbia Business School
USA
jerath@columbia.edu

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Marketing

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

W. J. Choi and K. Jerath. *Privacy and Consumer Empowerment in Online Advertising*. Foundations and Trends® in Marketing, vol. 15, no. 3, pp. 153–212, 2022.

ISBN: 978-1-68083-921-0

Foundations and Trends® in Marketing
Volume 15, Issue 3, 2022

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Marketing publishes survey and tutorial articles in the following topics:

- B2B Marketing
- Bayesian Models
- Behavioral Decision Making
- Branding and Brand Equity
- Channel Management
- Choice Modeling
- Comparative Market Structure
- Competitive Marketing Strategy
- Conjoint Analysis
- Customer Equity
- Customer Relationship Management
- Game Theoretic Models
- Group Choice and Negotiation
- Discrete Choice Models
- Individual Decision Making
- Marketing Decisions Models
- Market Forecasting
- Marketing Information Systems
- Market Response Models
- Market Segmentation
- Market Share Analysis
- Multi-channel Marketing
- New Product Diffusion
- Pricing Models
- Product Development
- Product Innovation
- Sales Forecasting
- Sales Force Management
- Sales Promotion
- Services Marketing
- Stochastic Model

Information for Librarians

Foundations and Trends® in Marketing, 2022, Volume 15, 4 issues. ISSN paper version 1555-0753. ISSN online version 1555-0761. Also available as a combined paper and online subscription.

Contents

Privacy and Consumer Empowerment in Online Advertising

W. Jason Choi[1] and Kinshuk Jerath[2]

[1] *Assistant Professor of Marketing, Rutgers Business School, USA; jason.choi@rutgers.edu*

[2] *Professor of Business, Marketing Division, Columbia Business School, USA; jerath@columbia.edu*

ABSTRACT

With heightened concerns regarding user privacy, there is a recent movement for empowering consumers with the ability to control how their private data are collected, stored, used and shared. Notably, between 2018 and 2020, the General Data Protection Regulation (GDPR) has been implemented in the European Union (EU), and the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) have been implemented/passed in the state of California in the United States. These regulations address both consumer data security and consumer privacy rights. In this monograph, we provide an overview of some of the key issues that are in play in consumer privacy and in empowering consumers with rights to manage the privacy of their data, viewed primarily in the context of online advertising-related actions of firms. The recent academic work on these topics already provides some important takeaways. Empirical studies, broadly speaking, show that fewer consumers share data with firms post-regulation and this

W. Jason Choi and Kinshuk Jerath (2022), "Privacy and Consumer Empowerment in Online Advertising", Foundations and Trends® in Marketing: Vol. 15, No. 3, pp 153–212. DOI: 10.1561/1700000053.

leads to worse personalized marketing, i.e., the firms are at a handicap. Theoretically, a primary insight is that privacy regulations on using data affect the advertising/targeting layer directly and the product/pricing layer directly and/or indirectly; broadly speaking, consumers make data sharing choices by balancing the intrinsic and instrumental values of sharing data, and privacy regulations can generally be expected to benefit consumers at the expense of firms. We also discuss how consumers' understanding of firms' privacy policies and their impact can be enhanced, which is important for regulations to have their intended impact. We briefly discuss the development of privacy-preserving mechanisms for targeted advertising, industry interest in and adoption of which has been recently enhanced due to new regulations. We conclude with a discussion and lay out some directions for future research.

Keywords: online advertising; privacy regulation; GDPR; consumer consent; targeting.

1

Introduction

The last 25 years have seen a consistent move by consumers to digital media. According to eMarketer, in 2019, the average American spent approximately seven hours a day on digital media, with approximately four hours of (non-voice) mobile phone consumption; in contrast, the total time spent per day on TV was 3.5 hours and on print media was 20 minutes.[1] Chasing consumers' media consumption habits, advertising dollars have also moved online. According to eMarketer, of the USD 242 billion spent on ads in the US in 2019, nearly 55% was on digital channels and less than 30% was on traditional linear TV.[2] Worldwide numbers in advertising spend show similar trends.[3]

A key promise of digital media is accurate targeting of ad prospects. In display advertising, which in 2019 accounted for more than 50% of digital ad spend (USD 71 billion out of USD 132 billion spent on digital

[1] https://forecasts-na1.emarketer.com/584b26021403070290f93a5d/5851918b0626310a2c186b38.

[2] https://forecasts-na1.emarketer.com/584b26021403070290f93a2f/5851918b0626310a2c186b4c.

[3] https://forecasts-na1.emarketer.com/5a4d1e53d8690c01349716b8/5a4d1bcfd8690c01349716b6 and https://forecasts-na1.emarketer.com/5d02b4e464fe7d06246b35f9/5d02b41c64fe7d06246b35f7.

advertising),[4] this targeting is enabled by developing profiles of users that can then be used to identify them as relevant matches for ads of certain products. Consumers often share their own information, such as their name, date of birth, interests and preferences, financial information, credit card data, credit score data, etc., with certain websites that they visit and (presumably) trust. However, a large fraction of the data used for building user profiles is collected by tracking consumers' activities on the Internet using technologies such as cookies and beacons—how often are consumers active on the Internet, which websites (and which parts of these websites) they visited, which products they browsed and purchased (or browsed and did not purchase), which geographical regions they come from, etc.

According to Schelter and Kunegis (2018), 355 third-party domains had installed trackers on over 90% of 41 million websites that they studied. Moreover, a recent study by Karaj *et al.* (2019) shows that 82% of the monitored web traffic had third-party scripts owned by Google, making it the largest third-party tracker by reach. While consumer tracking has benefited advertisers (Goldfarb and Tucker, 2011a; Johnson *et al.*, 2020), its rapid expansion has deepened consumers' concerns about their online privacy (McDonald and Cranor, 2010). For instance, 79% of US adults state that they are very or somewhat concerned about how companies are using the data they collect about them and 81% of US adults think that the potential risks of data collection by companies about them outweigh the benefits (PEW, 2019).

In response to the growing outcry from consumers and privacy advocates about the extent of consumer tracking and data collection, there is a movement for empowering consumers with the ability to control how their own data is collected, stored, used and shared. Certain advertising organizations and regulators worldwide have also sought to curb practices that potentially infringe on privacy. Notably, in May 2018, the General Data Protection Regulation (GDPR) came into force in the European Union (EU). Compared to its predecessors (e.g., Privacy and Electronic Communications Directive), the GDPR is considered

[4] https://forecasts-na1.emarketer.com/584b26021403070290f93a56/5851918a0626310a2c1869ca.

significantly more stringent and comprehensive in terms of geographic and legislative scope. The regulation applies to all firms processing personal data of European subjects even if the firm operates outside of Europe. Its hefty violation fines (the larger of $22.5 million and 4% of annual global turnover) are forcing large and small firms to take compliance seriously.[5] The California Consumer Privacy Act (CCPA), a US analogue of the GDPR and similar to it in many respects, was signed into law in June 2018 and came into effect in January 2020. In November 2020, the California Privacy Rights Act (CPRA), which modified certain aspects of the CCPA, was approved by California voters.

While consumers were able to delete cookies manually or through their web browser settings even before the regulations were active, complete tracking prevention was difficult (Angwin, 2010; Stern, 2018). Moreover, firms were able to purchase personal data from third-party information vendors without consumers' consent. In this context, the two main tenets of the GDPR are the requirements that firms: (a) inform consumers what data will be collected for what purposes, and (b) obtain explicit affirmative consent to use their data. In other words, firms are not allowed to collect consumer data by default; consumers themselves must consent to their data being collected and processed by firms. If consumers do not consent to their data being collected and shared, then advertisers cannot effectively monitor consumers' behavior across websites. Consequently, advertisers' targeting capabilities are drastically undermined and ad impressions could be potentially wasted (e.g., repeated exposure to consumers who had already purchased).[6] On the other hand, if consumers consent to their data being collected and shared, advertisers can target ads to specific audiences based on a set of behavioral criteria (e.g., consumers who previously interacted with the ad but did not purchase).

[5] In January 2019, Google was fined $57 million "for not properly disclosing to users how data is collected across its services . . . to present personalized advertisements" (Satariano, 2019). Facebook revamped their privacy settings in compliance with the GDPR (https://marketingland.com/what-marketers need-to-know-about-facebooks-updated-business-tools-terms-238140).

[6] https://www.blog.google/products/marketingplatform/360/privacy-safe-approach-managing-ad-frequency/.

The impact on the advertising industry of such privacy regulations that empower consumers is a topic of ongoing debate among practitioners, academics, and policymakers.[7] In this monograph, we provide an overview of the different issues that are in play in consumer privacy and in empowering consumers with rights to manage the privacy of their data, viewed primarily in the context of online advertising-related actions of firms. This is an emerging topic in both industry and academia, and therefore the existing work on it is relatively thin; nevertheless, some fundamental frameworks for thinking through the issues have already emerged. We review the existing knowledge on this topic and discuss implications for consumers, for advertisers (who we will assume are vertically integrated with the sellers of the product or service advertised), and for ad serving platforms that enable advertisers to reach consumers. As mentioned, our focus is on consumer privacy and consent in the context of digital marketing; for a discussion of privacy in a broader context, we refer the reader to Acquisti *et al.* (2015, 2016).

We note that privacy preservation can be of two types (Acquisti *et al.*, 2016): (1) privacy as protection against undesirable access of personal information, i.e., securely storing data collected from consumers (which falls under the umbrella of "data security"), and (2) privacy as control over collection and usage of consumer data, i.e., whether or not to obtain consumer data and how to use it (which falls under the umbrella of "privacy rights"). The second can also be thought of as consumers deciding whether to share or not share their data with a firm and determining how their shared data may be used. Furthermore, data can be of two types: (1) personal data, which includes sensitive data such as a consumer's name, Social Security Number, credit card number, home address, occupation, etc., and (2) behavioral data, which includes data such as how often a consumer is active on the Internet, which websites (and which parts of these websites) they visited, which products

[7] To the extent that consumers do not like to see ads, especially targeted ads, and do not want to be exposed to them, they can use ad blocking tools. Given the focus of this monograph, we do not look at the phenomenon of ad blocking in depth as it is beyond the scope of our discussion. However, some relevant papers for the interested reader are Anderson and Gans (2011), Johnson (2013), Gritckevich *et al.* (2019), Shiller *et al.* (2019) and Despotakis *et al.* (2020).

they browsed and purchased (or browsed and did not purchase), etc. In this monograph, in terms of privacy preservation our focus will be on privacy as control over usage and access. In terms of data, our focus will be on data that helps to contribute towards building a consumer profile, which includes both personal data and behavioral data, but the latter is typically of greater relevance for this purpose (Rafieian and Yoganarasimhan, 2021).

In this introductory section, we provide an outline of this monograph and briefly review the key ideas. In Section 2, we discuss the key aspects of, and the similarities and differences between, the GDPR, the CCPA and the CPRA.

Since the implementation of the GDPR in May 2018, some early empirical evidence has emerged of its impact. We review this evidence in Section 3. With respect to one of the most prominent aspects of the GDPR, which is consumers obtaining the right to not share their data with service providers, Aridor *et al.* (2020) and Goldberg *et al.* (2021) find that a significant minority of consumers prefer to opt out of data sharing. Interestingly, Godinho de Matos and Adjerid (2021) find that consumers with an existing relationship with a firm may be induced to provide consent for their data to be used for personalized marketing. Other papers, such as Johnson *et al.* (2021), show that privacy regulations may have unintended consequences such as hurting smaller service-provision firms (Johnson *et al.*, 2021) and hurting innovation (Janssen *et al.*, 2021 and Jia *et al.*, 2021).

In the last few years, there have been significant advances in our theoretical understanding of the impact of consumer privacy regulation on online advertising and on markets in general. A theoretical framework that helps to guide our understanding and study of consumer privacy is based on the idea that consumers attach value to different aspects of privacy. Specifically, consumers may attach value to privacy as a final good, i.e., with intrinsic value, and/or attach value to privacy as an intermediate good, i.e., with instrumental value (Becker, 1980; Posner, 1981; Wathieu and Friedman, 2009). The intrinsic value may arise simply from the effect that a consumer is not comfortable if other entities have their data and/or might be concerned that this data may be breached. The instrumental value of privacy may arise from the fact

that a consumer's data may be used by other entities to impact their experience and utility, e.g., by showing them highly relevant ads (which would improve experience and increase utility, all else equal) or price discriminating for them (which may decrease or increase utility).

To further understand the instrumental value of privacy, a useful economic framework that is to understand the impact of a consumer giving up privacy, i.e., a consumer sharing data, on the advertising market and on the product market. Broadly speaking, more data enables better targeting of consumers by firms in the advertising market which, under different conditions, can increase or decrease competition among the firms in the product market. Consumers can make their data sharing choices under these considerations, which in turn impacts the outcomes in the advertising and product markets. We review the privacy and economic frameworks in Section 4.

In Section 5, we enhance our understanding of the impact of privacy regulation on consumers and on online advertising by discussing the theoretical work in this area. Choi *et al.* (2020) show how firms can use consumer data to moderate product market competition through targeted informative advertising in the advertising market, which induces consumers to opt out of data sharing to increase their utility. D'Annunzio and Russo (2020) show that prevention of data sharing by consumers makes ad allocation less effective which can hurt consumers, i.e., regulation can hurt consumers. However, Choi *et al.* (2021) show that if the number of ads shown to be decided endogenously, then privacy regulation is weakly beneficial to consumers. Indeed, in reality, ads are not served in all possible impressions and ad fill rates can be significantly below 100%.[8]

A number of other papers do not model advertising directly but study consumer privacy choices in a context in which firms can obtain customer data, build customer profiles, and change the product offerings to consumers as well as the prices of these offerings. These papers include

[8] https://medium.com/@olssonm/have-your-adsense-coverage-plummeted-heres-why-1c284cb12bdc; https://smartyads.com/blog/ways-to-keep-your-ad-network-fill-rate-close-to-100/; https://twitter.com/jamesdutton/status/1136815781663072257; https://www.quora.com/What-is-the-sell-through-rate-of-ad-impressions-on-programmatic-exchanges/answer/Andre-Atomx.

Conitzer *et al.* (2012), Campbell *et al.* (2015), Anderson *et al.* (2019), D'Annunzio and Russo (2020), Montes *et al.* (2019), Choi *et al.* (2021), Ichihashi (2020), Ke and Sudhir (2020) and Sharma *et al.* (2021). The key take away from these studies is that privacy regulation generally helps consumers by preventing sharing of data when such sharing might hurt them, primarily through price discrimination; however, privacy regulation may hurt smaller publishers, advertisers and ad networks.

Studies have shown that when consumers are presented with privacy notices, they may not be able to fully understand them because of technical jargon and extensive length (Jensen and Potts, 2004; Jensen *et al.*, 2005; McDonald and Cranor, 2008). One could use a "revealed preference" argument to state that if consumers are making chocies based on these notices, they must be comfortable with the exchange of value (even with their potentially limited understanding of the notices). Nevertheless, there have been recent efforts to build tools that can help consumers to understand privacy policies of companies. One such effort is the Usable Privacy Project[9] which uses natural language processing and crowdsourcing to help train models that can then parse privacy policies and summarize them for consumers in a form that is easier to understand. On these lines, the development of a "privacy nutrition label" might be useful for consumers. We discuss these ideas in more details in Section 6.

Firms attach value to consumers' data and, starting with Laudon (1996), there has been talk of a marketplace where consumers and firms can transact in the consumers' data. We discuss this in Section 7. We also discuss recent attempts at this in the form of intermediaries, such as the Brave browser, that share a portion of the revenues that they generate from consumer data with the consumers themselves.

In light of the passing of privacy regulation, firms have been attempting to develop methods for privacy-preserving targeted advertising, which essentially is advertising that does not use cookies to build profiles of and target consumers. In Section 8, we discuss some of these attempts such as FLoC and TURTLEDOVE, which aim to target consumers based on their interests and/or their website visit history, but without

[9] https://www.usableprivacy.org/.

compromising their privacy. At the time of this writing, all of these methodologies were in the proposal or testing stages.

Finally, in Section 9, we conclude with a discussion. An overall summary is that privacy concerns have been heightened in the past two decades and this has led to the passing of privacy regulations addressing data security and privacy rights. After these regulations, a significant minority of consumers have chosen to not provide consent for their data to be collected, used and shared. However, most consumers still may not properly understand the key implications of privacy policies of firms, and more efforts are needed in that regard. Also, technologies are being developed for privacy-preserving user targeting. Finally, regarding firms, data frictions caused by privacy regulations have, in turn, caused (presumably unintended) negative consequences for small advertisers, publishers and service providers. We provide some directions for future work that may be valuable to move thinking forward on this increasingly important topic.

References

Acemoglu, D., A. Makhdoumi, A. Malekian, and A. Ozdaglar (2019). "Too much data: Prices and inefficiencies in data market". *Working Paper*. National Bureau of Economic Research.

Acquisti, A., L. Brandimarte, and G. Loewenstein (2015). "Privacy and human behavior in the age of information". *Science*. 347(6221): 509–514.

Acquisti, A., L. John, and G. Loewenstein (2013). "What is privacy worth?" *Journal of Legal Studies*. 42(2): 249–274.

Acquisti, A., C. Taylor, and L. Wagman (2016). "The economics of privacy". *Journal of Economic Literature*. 54(2): 442–492.

Anderson, S., A. Baik, and N. Larson (2019). "Prices, poaching, and privacy with personalized targeted discounts". *Working Paper*.

Anderson, S. and J. Gans (2011). "Platform siphoning: Ad-avoidance and media content". *American Economics Journal: Microeconomics*. 3(November): 1–34.

Angwin, J. (2010). "The Web's new gold mine: Your secrets". *The Wall Street Journal*.

Argenziano, R. and A. Bonatti (2021). "Data linkages and privacy regulation". *Working Paper*.

Aridor, G., Y.-K. Che, and T. Salz (2020). "The economic consequences of data privacy regulation: Empirical evidence from GDPR". *Working Paper*.

Athey, S., C. Catalini, and C. Tucker (2017). "The digital privacy paradox: Small money, small costs, small talk". Technical report, National Bureau of Economic Research.

Aziz, A. and R. Telang (2016). "What is a digital cookie worth?" *Working Paper*.

Becker, G. S. (1980). "Privacy and malfeasance: A comment". *Journal of Legal Studies*. 9(4): 823–826.

Bergemann, D. and A. Bonatti (2011). "Targeting in advertising markets: Implications for offline versus online media". *RAND Journal of Economics*. 42(3): 417–443.

Campbell, J., A. Goldfarb, and C. Tucker (2015). "Privacy regulation and market structure". *Journal of Economics and Management Strategy*. 24(1): 47–73.

Chen, Y., X. Hua, and K. E. Maskus (2021). "International protection of consumer data". *Journal of International Economics*. 132: 103517.

Choi, J., K. Jerath, and M. Sarvary (2020). "Advertising and price competition under consumer privacy data choices". *Working Paper*.

Choi, J., K. Jerath, and M. Sarvary (2021). "Consumer purchase journey, ad wearout and privacy choices". *Working Paper*.

Conitzer, V., C. Taylor, and L. Wagman (2012). "Hide and seek: Costly consumer privacy in a market with repeat purchases". *Marketing Science*. 31(2): 277–292.

D'Annunzio, A. and A. Russo (2020). "Ad networks and consumer tracking". *Management Science*. 66(11): 5040–5058.

de Corniére, A. and R. de Nijs (2016). "Online advertising and privacy". *RAND Journal of Economics*. 47(1): 48–72.

de Corniére, A. and R. Montes (2017). "Consumer privacy and the incentives to price-discriminate in online markets". *Review of Network Economics*. 16(3): 291–305.

Degeling, M., C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz (2019). "We value your privacy . . . now take some cookies: Measuring the GDPR's impact on web privacy". In: *26th Annual Network and Distributed System Security Symposium (NDSS '19)*. Internet Society.

Despotakis, S., R. Ravi, and K. Srinivasan (2020). "The beneficial effects of ad blockers". *Management Science*. 67(4): 2096–2125.

Esteves, R. (2010). "Pricing with customer recognition". *International Journal of Industrial Organization*. 28(6): 669–681.

Esteves, R.-B. and J. Resende (2016). "Competitive targeted advertising with price discrimination". *Marketing Science*. 35(4): 576–587.

Farrell, J. (2012). "Can privacy be just another good?" *Journal on Telecommunications and High Technology Law*. 10(2): 251–264.

Fudenberg, D. and J.-M. Villas-Boas (2012). "Price discrimination in the digital economy". In: *The Oxford Handbook of the Digital Economy*. Ed. by M. Peitz and J. Waldgofel. Oxford, UK: Oxford University Press. 254–272.

Gaelotti, A. and J. L. Moraga-Gonzalez (2008). "Advertising, segmentation and prices". *International Journal of Industrial Organization*. 26(5): 1106–1119.

Godinho de Matos, M. and I. Adjerid (2021). "Consumer consent and firm targeting after GDPR: The case of a large telecom provider". *Management Science*. Forthcoming.

Goldberg, S., G. Johnson, and S. Shriver (2021). "Regulating privacy online: An economic analysis of the GDPR". *Working Paper*.

Goldfarb, A. and C. Tucker (2011a). "Online display advertising: Targeting and obtrusiveness". *Marketing Science*. 30(3): 389–404.

Goldfarb, A. and C. Tucker (2011b). "Privacy regulation and online advertising". *Management Science*. 57(1): 57–71.

Goldfarb, A. and C. Tucker (2012). "Shifts in privacy concerns". *American Economic Review*. 102(3): 349–353.

Gritckevich, A., Z. Katona, and M. Sarvary (2019). "Ad blocking". *Working Paper*.

Ichihashi, S. (2020). "Online privacy and information disclosure by consumers". *American Economic Review*. 110(2): 569–595.

Ipsos (2019). "Global citizens and data privacy". URL: https://bit.ly/3hwpWAT.

Iyer, G., D. Soberman, and J. M. Villas-Boas (2005). "The targeting of advertising". *Marketing Science*. 24(3): 461–476.

Janssen, R., R. Kesler, M. Kummer, and J. Waldfogel (2021). "GDPR and the lost generation of innovative apps". *Working Paper*.

Jensen, C. and C. Potts (2004). "Privacy policies as decision-making tools: An evaluation of online privacy notices". In: *SIGCHI Conference on Human Factors in Computing Systems, ACM*. Vienna. 471–478.

Jensen, C., C. Potts, and C. Jensen (2005). "Privacy practices of Internet users: Self-reports versus observed behavior". *International Journal of Human Computer Studies*. 63(1–2): 203–227.

Jia, J., G. Jin, and L. Wagman (2021). "The short-run effects of GDPR on technology venture investment". *Marketing Science*. 40(4): 661–684.

Johnson, E. J., S. Bellman, and G. L. Lohse (2002). "Defaults, framing and privacy: Why opting in-opting out". *Marketing Letters*. 13(1): 5–15.

Johnson, G., S. Shriver, and S. Du (2020). "Consumer privacy choice in online advertising: Who opts out and at what cost to industry?" *Marketing Science*. 39(1): 33–51.

Johnson, G., S. Shriver, and S. Goldberg (2021). "Privacy and market concentration: Intended and unintended consequences of the GDPR". *Working Paper*.

Johnson, J. P. (2013). "Targeted advertising and advertising avoidance". *RAND Journal of Economics*. 44(1): 128–144.

Karaj, A., S. Macbeth, R. Berson, and J. M. Pujol (2019). "Who tracks me: Shedding light on the opaque world of online tracking". arXiv preprint arXiv:1804.08959.

Ke, T. T. and K. Sudhir (2020). "Privacy rights and data security: GDPR and personal data driven markets". *Working Paper*.

Kostov, N. and S. Schechner (2018). "Google emerges as early winner from Europe's new data privacy law". *Wall Street Journal*.

Kummer, M. and P. Schulte (2019). "When private information settles the bill: Money and privacy in Google's market for smartphone applications". *Management Science*. 65(8): 3470–3494.

Laudon, K. (1996). "Markets and privacy". *Communications of the ACM*. 39(9): 92–104.

Libert, T. (2018). "An automated approach to auditing disclosure of third-party data collection in website privacy policies". In: *Proceedings of the 2018 World Wide Web Conference on World Wide Web (2018), International World Wide Web Conferences Steering Committee*. 207–216.

Lin, T. (2020). "Valuing intrinsic and instrumental preferences for privacy". *Working Paper*.

McDonald, A. M. and L. F. Cranor (2008). "The cost of reading privacy policies". *I/S: A Journal of Law and Policy for the Information Society*. 4: 540–565.

McDonald, A. M. and L. F. Cranor (2010). "Americans' attitudes about Internet behavioral advertising practices". In: *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society*. ACM. 63–72.

Montes, R., W. Sand-Zantman, and T. Valletti (2019). "The value of personal information in online markets with endogenous privacy". *Management Science*. 65(3): 1342–1362.

Norberg, P. A., D. R. Horne, and D. A. Horne (2007). "The privacy paradox: Personal information disclosure intentions versus behaviors". *Journal of Consumer Affairs*. 41(1): 100–126.

Nouwens, M., I. Liccardi, M. Veale, D. Karger, and L. Kagal (2020). "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence". In: *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

PEW (2019). "Americans and privacy: Concerned, confused and feeling lack of control over their personal information". URL: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Posner, R. A. (1981). "The economics of privacy". *American Economic Review*. 71(2): 405–409.

Rafieian, O. and H. Yoganarasimhan (2021). "Targeting and privacy in mobile advertising". *Marketing Science*. 40(2): 193–218.

Roy, S. (2000). "Strategic segmentation of a market". *International Journal of Industrial Organization*. 18(8): 1279–1290.

Satariano, A. (2019). "Google is fined $57 million under Europe's data privacy law". *The New York Times*.

Schelter, S. and J. Kunegis (2018). "On the ubiquity of web tracking: Insights from a billion-page web crawl". *The Journal of Web Science*. 4(4): 53–66.

Sharma, P., Y. Sun, and L. Wagman (2021). "The differential effects of privacy protections and digital ad taxes on publisher and advertiser profitability". *Working Paper*.

Shelanski, H. A. (2013). "Information, innovation and competition policy for the Internet". *University of Pennsylvania Law Review*. 161: 1663–1705.

Shen, Q. and J. M. Villas-Boas (2018). "Behavior-based advertising". *Management Science*. 64(5): 2047–2064.

Shiller, B., J. Waldfogel, and J. Ryan (2019). "The effect of ad blocking on website traffic and quality". *RAND Journal of Economics*. 49(1): 34–63.

Slovic, P. (1995). "The construction of preference". *American Psychologist*. 50(5): 364–371.

Stern, J. (2018). "Facebook really is spying on you, just not through your phone's mic". *Wall Street Journal*.

Sun, T., Z. Yuan, C. Li, K. Zhang, and J. Xu (2020). "The value of personal data in Internet commerce: A high-stake field experiment on data regulation policy". *Working Paper*.

Taylor, C. and L. Wagman (2014). "Consumer privacy in oligopolistic markets: Winners, losers, and welfare". *International Journal of Industrial Organization*. 34(1): 80–84.

Utz, C., M. Degeling, S. Fahl, F. Schaub, and T. Holz (2019). "(Un)informed consent: Studying GDPR consent notices in the field". In: *CCS'19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 973–990.

Villas-Boas, J. M. and Y. Yao (2021). "A dynamic model of optimal retargeting". *Marketing Science*. Forthcoming.

Wathieu, L. and A. Friedman (2009). "An empirical approach to understanding privacy concerns". *Working Paper*.

Xu, H., H. Teo, C. Tan, and R. Agarwal (2010). "The role of push-pull technology in privacy calculus: The case of location-based services systems". *Journal of Management Information*. 26(3): 137–176.