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

*Brands: An Integrated Marketing, Finance, and Societal Perspective*
Bobby J. Calder

*Machine Learning in Marketing: Overview, Learning Strategies, Applications, and Future Developments*
Vinicius Andrade Brei

*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
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
ISBN: 978-1-68083-921-0
© 2022 W. J. Choi and K. Jerath

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The ‘services’ for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Full text available at: http://dx.doi.org/10.1561/1700000053
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

1 Introduction 3

2 A Background of the GDPR, CCPA and CPRA Regulations 11

3 Early Empirical Evidence on Impact of Enabling Consumer Privacy Choices 14

4 Frameworks for Understanding Consumer Privacy Decisions and Their Economic Impact 18
   4.1 Framework for Privacy 18
   4.2 Framework for Economic Impact 20

5 Theoretical Understanding of the Impact of Enabling Consumers to Make Privacy Choices 23
   5.1 Impact on the Advertising Ecosystem of Enabling Consumers to Make Privacy Choices 23
   5.2 Impact on Consumers of Enabling Consumers to Make Privacy Choices 34

6 Enabling Users to Make Better Privacy Choices 36

7 Markets for Personal Data 43
Privacy and Consumer Empowerment in Online Advertising

W. Jason Choi\textsuperscript{1} and Kinshuk Jerath\textsuperscript{2}

\textsuperscript{1}Assistant Professor of Marketing, Rutgers Business School, USA; jason.choi@rutgers.edu
\textsuperscript{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
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.
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](https://forecasts-na1.emarketer.com/584b26021403070290f93a5d/5851918b0626310a2c186b38).

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

\(^3\) [https://forecasts-na1.emarketer.com/5a4d1e53d8690c01349716b8/5a4d1bcfd8690c01349716b6](https://forecasts-na1.emarketer.com/5a4d1e53d8690c01349716b8/5a4d1bcfd8690c01349716b6) and [https://forecasts-na1.emarketer.com/5d02b41e64fe7d06246b35f9/5d02b41e64fe7d06246b35f7](https://forecasts-na1.emarketer.com/5d02b41e64fe7d06246b35f9/5d02b41e64fe7d06246b35f7).
advertising), 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

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. 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). 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).

5In 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).
The impact on the advertising industry of such privacy regulations that empower consumers is a topic of ongoing debate among practitioners, academics, and policymakers. 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

---

7To 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), Gritkevich 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%.

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

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 choices 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

---

\(^9\)\url{https://www.usableprivacy.org/}. 

Full text available at: http://dx.doi.org/10.1561/1700000053
Introduction

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.


Full text available at: http://dx.doi.org/10.1561/1700000053


