AN A.S. PRATT PUBLICATION
MAY 2017
VOL. 3 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 4 | MAY 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [129] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Are You Exposing Your Company to Liability by Using Cross-Device Tracking Data?

By Nicholas R. Merker and Blaine L. Dirker*

Consumers may not realize that their browsing behavior and account accesses can be monitored across multiple devices, commonly referred to as cross-device tracking. The authors of this article explain cross device tracking, the privacy concerns, and recent guidelines and self-regulatory initiatives to address such privacy concerns.

As internet connected mobile devices (e.g., smartphones, laptops, tablets, wearables, smart appliances, etc.) have become seemingly ubiquitous, consumers now have more ways than ever to access the internet to interface with social media accounts, check email, purchase goods and services, seek medical advice, watch cat videos, etc. However, consumers may not realize that such browsing behavior and account accesses can be monitored. Traditional browser tracking methods, such as web cookies and local shared objects, have typically not been as reliable in the mobile space. As such, the traditional methods are being replaced or supplemented with a method for tracking consumer behavior across multiple devices, commonly referred to as cross-device tracking.

In practice, various entities (e.g., service providers, content publishers, advertising companies, etc.) actively monitor consumer behavior, both online and offline, to generate detailed profiles of consumers. Cross-device tracking allows companies to further refine such profiles using data gathered for consumers across more than one of their devices. For example, a consumer may browse a particular vendor's website for an article of clothing via a web browser on their tablet, and an advertisement for that same vendor and/or article of clothing may show up in their social media feed accessed on their smartphone.

TWO MAIN APPROACHES TO CROSS-DEVICE TRACKING

Advertisers typically rely on two main approaches to cross-device tracking: deterministic matching and probabilistic matching. Deterministic matching relies on some explicit identification by the consumer themselves, such as a username, email address, mobile phone number, etc. Probabilistic matching methods may be used to associate the consumer between their devices by using device information, such as the operating system, device make and model, IP address, etc. For example, if both devices have accessed content using the same IP address, one can make a calculated guess that the same consumer is using both devices. Further, if both devices have been used to access

* Nicholas R. Merker is a partner at Ice Miller LLP and co-chair of its Data Security and Privacy Practice. Blaine L. Dirker is of counsel in the firm's Intellectual Property and Data Security and Privacy practices. The authors may be reached at nicholas.merker@icemiller.com and blaine.dirker@icemiller.com, respectively.

the same email address, a stronger inference can be made that both devices are associated with the same consumer.

PRIVACY CONCERNS

While cross-device tracking can provide certain benefits to the user, such as in the form of a seamless experience across devices and applications, and provide a level of fraud protection and account security, cross-device tracking also presents a number of privacy concerns. As the International Association of Privacy Professionals ("IAPP") noted in their practice guide to cross-device tracking, "[t]he variety of technologies used for cross-device tracking creates challenges for consent, notice, and opt-out standards."[1] For example, the data gathered as a result of monitoring consumer behavior can be stored, aggregated, and analyzed by various entities, all unbeknownst to the consumer. As a result, government agencies and industry trade groups alike have introduced guidelines and self-regulatory initiatives to address such privacy concerns.

GUIDELINES AND SELF-REGULATORY INITIATIVES TO ADDRESS PRIVACY CONCERNS

In one such example, in May 2015, the Network Advertising Initiative ("NAI"), an industry trade group of third party network advertisers that develops self-regulatory standards for online advertising, introduced their Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI Code of Conduct.[2] The NAI Guidance covers, among other things, the transparency and notice requirements for NAI Members. In particular, the NAI Guidance requires that for non-cookie technology, the privacy policy include whether data is being collected using a non-cookie technology and a description of an easy-to-use opt-out mechanism which allows consumers to opt-out of Internet-Based Advertising ("IBA") with respect to a particular browser or device.

Another such example is from the Digital Advertising Alliance ("DAA"), an independent non-profit organization led by the leading advertising and marketing trade associations, which released specific guidance on the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices[3] – enforcement

[1] https://iapp.org/resources/topics/cross-device-tracking/.

[2] NETWORK ADVERT. INITIATIVE, GUIDANCE FOR NAIMEMBERS: USE OF NON-COOKIE TECHNOLOGIES FOR INTEREST-BASED ADVERTISING CONSISTENT WITH THE NAI CODE OF CONDUCT 2 (2015) ("Beyond Cookies") *available at* http://www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf.

[3] DIG. ADVERT. ALL., APPLICATION OF THE SELF-REGULATORY PRINCIPLES OF TRANSPARENCY AND CONTROL TO DATA USED ACROSS DEVICES 2 (2015), *available at* http://www.aboutads.info/DAA_Cross-Device_Guidance-Final.pdf.

of which began on February 1, 2017.[4] Similar to the NAI Guidance, the DAA's Principles require an opt-out mechanism; however, the DAA's Principles further require a disclosure that lists all third parties engaged in the collection of cross-device tracking data. Additionally, in accordance with the DAA's Principles, data collected from an opted-out device cannot be used for behavioral advertising on other devices, nor can data collected from other devices inform advertising on the opted-out device.

More recently, in January 2017, the Federal Trade Commission ("FTC") released a Staff Report detailing the findings of a Cross-Device Tracking Workshop conducted by the FTC in November 2015. Research undertaken by the FTC concluded that an increasing number of companies have advertised using cross-device tracking services. To that end, the FTC Staff Report provided the following recommendations for those companies engaged in cross device tracking:

- be *transparent* about data collection and use practices;
- provide *choice* mechanisms that give consumers control over their data;
- provide *heightened protections* for sensitive information, including health, financial, and children's information; and
- maintain *reasonable security* of collected data.

Further, the FTC Staff Report highlighted various circumstances in which cross-device tracking companies, publishers, and device manufacturers can run afoul of the FTC Act. Such circumstances that could implicate the FTC ACT can include:

- Failure to provide truthful information about tracking practices.[5]
- Failure to disclose cross-device tracking as a data collection/tracking method.[6]
- Failure to properly identify the types of information being collected and used.[7]
- Failure to clearly and conspicuously disclose the limits of an opt-out that is limited to only certain types of tracking technologies.[8]

To safeguard data collection practices associated with cross-device tracking, the FTC Staff Report advises companies to:

- Clearly and conspicuously disclose cross-device tracking practices by explaining to consumers what information is collected from the device, the entities that are

[4] Press Release, Dig. Advert. All., Digital Advertising Alliance Announces Enforcement of Cross-Device Guidance to Begin February 1, 2017 (Jan. 31, 2017), *available at* http://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-announces-enforcement-cross-device-guidance-begin.

[5] Epic Marketplace, Inc., No. C-4389 (F.T.C Mar. 13, 2013) (complaint), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacecmpt.pdf.

[6] Press Release, Fed. Trade Comm'n, FTC Issues Warning Letters to App Developers Using "Silverpush" Code (Mar. 17, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

[7] *United States v. InMobi Pte Ltd.*, No. 3:16-cv-3474 (N.D. Cal. June 22, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf.

[8] Beyond Cookies, *supra* note 2, at 9.

collecting the information, and how they use and share the information collected.

- Offer consumers choices about how their cross-device activity is shared, and respect those choices.
- Do not refer to raw or hashed usernames/email addresses as anonymous or aggregated data – the FTC has repeatedly held that data that is reasonably linked to a consumer or a consumer's device is personally identifiable. Accordingly, do not make blanket statements to consumers about not sharing "personal information" with third parties if such data is being shared.
- Refrain from engaging in cross-device tracking on data that the FTC has recognized as sensitive, warranting higher levels of protection, including health, financial, and children's information, as well as precise geolocation information, without the consumer's affirmative express consent.
- Take efforts to maintain reasonable security and properly secure data in order to avoid unexpected and/or unauthorized uses of data (e.g., as may be otherwise compromised via a data breach).

CONCLUSION

In summary, if your company uses data collected via cross-device tracking collection methods, be transparent about the data collected, how it is collected, and the intended use for the data. Additionally, allow consumers to have control over their data (e.g., opt-out mechanisms), recognize how collected and disseminated data collected via cross-device tracking can be classified (e.g., as personal information, sensitive data, etc.), and maintain reasonable security.