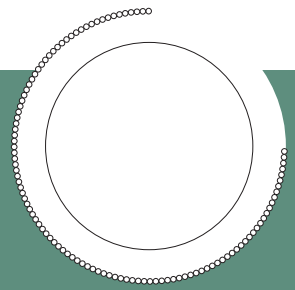


Cross-Device Tracking

An FTC Staff Report

January 2017

FEDERAL TRADE COMMISSION

Edith Ramirez, Chairwoman
Maureen K. Ohlhausen, Commissioner
Terrell McSweeny, Commissioner

Report Contributors

Bureau of Consumer Protection
Jessica Rich, Director, Bureau of Consumer Protection
Daniel Kaufman, Deputy Director, Bureau of Consumer Protection
Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection
Laura Riposo VanDruff, Assistant Director, Division of Privacy and Identity Protection
Megan Cox, Staff Attorney, Division of Privacy and Identity Protection
Ryan Mehm, Staff Attorney, Division of Privacy and Identity Protection
Justin Brookman, Policy Director, Office of Technology Research and Investigation
Aaron Alva, Tech Policy Fellow, Office of Technology Research and Investigation

Bureau of Economics
Andrew E. Stivers, Deputy Director, Bureau of Economics
Janis K. Pappalardo, Assistant Director, Bureau of Economics
Timothy P. Daniel, Deputy Assistant Director, Bureau of Economics

Contents

Executive Summary

The Federal Trade Commission has examined online behavioral advertising since the mid-1990s, when the internet first emerged as a commercial medium. Since then, the FTC has hosted workshops, issued reports, promoted self-regulation, and developed principles for the online behavioral advertising industry. Throughout this time, the FTC has worketnv2.7(c)-2.en

first-party services with a direct relationship with the consumer—for example, an email service that a consumer logs onto from different devices.[3] However, third-party companies are tracking consumers with increasing accuracy, correlating user behavior across multiple platforms.[4]

This report describes the FTC's November 2015 Cross-Device Tracking Workshop, which included discussions about how cross-device tracking works, the benefits and challenges of cross-device tracking, and industry efforts to address the privacy and security implications of this practice. It concludes by providing recommendations to businesses on how to apply the FTC's longstanding privacy principles to cross DevicTomgs3aJ [(7(i)-2(va)20(i

data to create detailed consumer profiles.[8] With cross-device tracking, tracking no longer occurs solely on a single computer or device.[9] Companies can gather information about consumers across their connected devices, including smartphones, tablets, personal computers, smart televisions, and even smartwatches and other wearables. Many of these companies hope to combine this information with information about consumers' offline habits.[10]

II. The Cross-Device Tracking Workshop

The Commission hosted the Cross-Device Tracking Workshop to explore the implications of this practice for consumers, and to determine how traditional principles, such as transparency, choice, and security apply. It also examined what self-regulatory organizations and companies were doing in this area. Based on information gathered through the workshop, this report describes: (1) the ways cross-device tracking technologies work; (2) the benefits and challenges of the practice; and (3) efforts by self-regulatory organizations to address cross-device tracking.

Cross-Device Tracking Technology

Through cross-device tracking, companies can associate multiple devices with the same person. While this information serves many purposes, it is particularly useful and valuable to advertisers.[11] For example, a consumer may purchase a pair of shoes on their smartphone after having been served an ad on their work computer. Cross-device tracking can help an advertiser determine that the consumer who made the purchase is the same consumer who saw the ad. Advertisers can use this type of information to measure the success of an ad campaign and avoid inundating consumers with the same ad. They can also use the information to target ads to a consumer, such as an ad for a belt to match the shoes. As the number of devic.

identifying characteristic, such as a login.[13] Consumers often take affirmative steps to identify themselves on each device they use, by logging into an account or using an e-mail address, for example.[14] Through that affirmative step, companies can associate a consumer's activity on one device with activity they observe on other devices associated with that account.[15] Many sites that offer a login also offer functionalities that can be embedded into other sites to track consumers—such as social sharing widgets, analytics code, social network logins, or advertising. For example, if a consumer logs into the same platform account on a desktop and smartphone, the consumer's query for blue jeans through that platform on her desktop browser can then inform the ads in a smartphone app that uses the same platform to serve targeted mobile ads.

Companies can also use a probabilistic approach to infer which consumer is using a device, even when a consumer has not logged into a service.[16] A common method of probabilistic tracking is IP address matching.[17] When an ad platform places a cookie on a consumer's browser, the cookie often includes the IP address of the device running the browser. Because devices on the same local network often have the same public IP address, the ad platform might infer that a computer, smartphone, and tablet that use the same public IP address belong to the same household. As another example, if a consumer's smartphone uses the same public IP address as her work computer during business hours, and then uses the same public IP address as her home computer during non-business hours, an ad platform might infer that the work computer, smartphone, and home computer belong to the same consumer. If the platform has access to geolocation information for the three devices, it may be able to ascribe more certainty to this inference. Additionally, a company might infer that a work smartphone and personal smartphone that visit the same unusual combination of websites belong to the same user.[18] Once a company has linked a consumer's devices in this manner, when that consumer books airline reservations to Hawaii on her home computer's browser, for example, she might see ads for hotels in Hawaii on her smartphone or work computer.

Because consumers do not have to be logged in to any service for companies to track them probabilisticly, this method of linking might be less apparent to consumers. Consumers generally have a relationship with deterministic platforms, choose to engage with these platforms, and can access the platforms' policies on data collection and data sharing to learn more about how their information or online behavior could be used. By contrast, probabilistic tracking companies, like third-

platforms generally, work with businesses out of consumers' view and rarely have direct consumer relationships.

To improve the accuracy of their cross-device tracking models, companies often combine deterministic and probabilistic techniques. Indeed, companies that have deterministic data, such as email providers, social networks, or shopping sites, frequently work with entities engaged in probabilistic tracking.[19] Suppose a consumer visits a retailer's shopping site on his work computer, a news website on his smartphone, and a video streaming service on his home computer, using the same email address to log into these separate services. These first-party sites (with deterministic data) may share hashed[20] email addresses with their partner ad network. With this unique identifier for each consumer, the third-party ad network can determine that the three devices noted in the example

16 of

Cross-device tracking provides companies with improved metrics that may help them avoid the over-saturation of ads.[31] It also enables them to deliver more relevant ads to consumers who may want them.[32] For example, marketers can see how ads influence purchases on different devices and target advertising to the consumers who are most likely to be interested in the advertisers' products.[33]

Finally, cross-device tracking technology may enhance competition in the advertising arena. Currently, few entities have large user bases with deterministic data (*e.g.*, login information) that they can use to track consumers across devices and serve ads.[34] By leveraging cross-device tracking technology, companies without deterministic data may be able to compete with first-party entities that do,[35] providing insights to clients,[36] forging new advertising models with a better consumer experience, and increasing efficiency to benefit those in the advertising ecosystem, including consumers.[37]

However, cross-device tracking also creates privacy challenges. The first challenge is transparency.[38] Because the practice of cross-device tracking is often not obvious, consumers may be surprised to find that their browsing behavior on one device will inform the ads they see on another device.[39] Indeed, many of the consumers who submitted comments to the workshop expressed concern about the practice

of cross-device tracking.[40] Probabilistic tracking, where consumers are tracked without having signed in to any service, may be particularly surprising and concerning to consumers, especially where sensitive information is involved. For example, a person may not expect that if she downloads an app related to a medical condition in the privacy of her home, she may receive ads on other platforms related to that condition.[41] A teen who does not want her parents to know she is gay may be surprised to learn that her browsing behavior on her mobile device informs ads that appear on the household computer.[42] As with all practices that implicate consumer privacy, when sensitive information is involved, there is a heightened need for transparency, choice, and security.

Consumers may also be unaware of the potential scope of cross-device tracking. Such practices may not be limited to tracking consumers across desktops, laptops, tablets and smartphones. It may also include viewing information from smart televisions, health information from a wearable device, or even shopping habits at brick-and-mortar stores.[43] Thus, a consumer could get an ad on her work computer related to a program she watched on television, habits revealed by her wearable device, or retail purchases.

---

[40] *See* Comment #18 from Susan Burstad, to Fed. Trade Comm'n (Apr. 20, 2015) ("I consider tracking from my devices the most insidious of invasion of privacy issues."), https://www.ftc.gov/policy/public-comments/2015/04/20/comment-00018; Comment #15 from Boonie McFadden, to Fed. Trade Comm'n (Apr. 12, 2015) ("Non-consensual tracking of my internet use must be ended. This is a gross invasion of privacy, and a violation of constitutional protections."), https://www.ftc.gov/policy/public-comments/2015/04/12/comment-00015; Comment #11 from Paula McMullan, to Fed. Trade Comm'n (March 22, 2015) ("My privacy is far more important to me than providing advertisers with a way to inundate me with more advertising. 'Relevant' advertising is a negative for me—not a positive."), https://www.ftc.gov/policy/public-comments/2015/03/22/comment-00011; Comment #10 from Ernst, to Fed. Trade Comm'n (March 20, 2015) ("I should not have to leave my smart phone in my car when I shop in order to prevent form of [*sic*] this abuse."), https://www.ftc.gov/policy/public-comments/2015/03/20/comment-00010; Comment #62 from Myles Lewis, to Fed. Trade Comm'n (Dec. 8, 2015) ("I find that Cross Device Tracking and its associated technologies to be a disturbing invasion of my personal privacy."), https://www.ftc.gov/policy/public-comments/2015/12/08/comment-00062; Comment #59 from Darin Gordon, to Fed. scn31(6 54 343.31(6 54 3( )Tj ET EMC BT /Link <</.5(r)-)6.9(d not) EMC B20/) B20/ec..n]TJ 0 006 Tc -0

Companies do not appear to be explicitly discussing cross-device tracking practices in their privacy policies.

reported that at least 419 million consumers, or 22% of the world's smartphone users, are blocking ads on the mobile web.[52] Another recent study inquired why people use ad blockers, and 39% of U.S.

This could be especially harmful for consumers in the banking sector, which has historically relied upon security questions about personal information.[59]

Industry Self-Regulatory Efforts to Address Cross-Device Tracking

At the workshop, participants discussed steps that NAI and DAA have taken to address cross-device tracking. In May 2015, the NAI released a guide for members, explaining how its Code of Conduct would apply to the use of non-cookie technologies.[60] Although the guidance does not update or amend the NAI's Code of Conduct, it sets forth baseline best practices for providing transparency about non-cookie technologies.[61] For example, it suggests that members describe the non-cookie tracking in their privacy policies and make a "reasonable effort" to ensure that their publisher-clients include information about it in their privacy policies.[62] NAI does not yet enforce compliance with the non-cookie tracking guidance it issued in May 2015.[63]

The DAA has addressed cross-device tracking more specifically. In August 2014, one of the DAA's enforcement organizations issued compliance warnings stating that the DAA Principles apply to both cookie tracking and non-cookie tracking, including tracking across devices and platforms.[64] In November 2015, the DAA released specific guidance on the application of DAA Principles to cross-device tracking, stating that the transparency and consumer control obligations in its existing Principles apply to cross-device tracking data practices.[65] According to DAA's 2015 guidance, if a consumer opts out of data collection for behavioral advertising on one device, the data collected from that device

---

[59] Antone Gonsalves, *Hack of Major Data Brokers Weakens Bank Authentication*, CSOONLINE (Sept. 27, 2013), http://www.csoonline.com/article/213400

tracking activities. Providing meaningful information to consumers about cross-device tracking will help consumers decide whether to use existing opt-out tools, whether to attempt to silo their activities, or whether to stop using a website, app, or service altogether.

As to the cross-device tracking companies, staff recommends that they provide truthful disclosures, to consumers *and* to the first-party companies on whose websites and apps they appear, so that these first parties can in turn make truthful disclosures to consumers. In some circumstances, failure to provide truthful information about tracking practices could violate the FTC Act. For example, in its action against the online advertising company Epic Marketplace, the Commission alleged that the company engaged in deceptive practices in violation of Section 5 of the FTC Act by making promises to consumers about the limited nature of its tracking when, in fact, it used "history sniffing" technology to track consumers across the internet.[71]

As consumer-facing companies, publishers and device manufacturers should also be transparent. In some cases, the failure of an app developer or website operator to disclose cross-device tracking could implicate the FTC Act. Staff recently sent warning letters to app developers who had allowed third parties to install 5 o,-0.004 Tc 0.0042Tw [(S)-2(d a)4wiw Tw 3.47 0 Td [3.7ckih-2(he)4(( )2(.t)-2(o dit)-2(e)4(d(or

consumer or a

receiving behavioral ads will also prevent data from that device from informing behavioral ads on other devices.[83] We encourage the NAI to do the same.

Although the DAA's new approach will allow consumers to opt out a single device from a device graph, consumers will still have to opt out on a device-by-device basis. Some have advocated for a single opt-out that would apply across consumers' browsers, smartphones, tablets, and smart devices.

However, we recognize that current limitations make it difficult to effectuate a single opt-out.[84] Ad tech companies may be concerned that single opt-outs will be imperfect and that they may not be able to correctly associate devices with individual consumers. A consumer who thinks she is opting out all of her devices might have a device she uses less frequently, which may result in the company not realizing that the device is part of the consumer's device graph. Accordingly, the company may continue to serve targeted ads to thatthatt a h (e i) u - s 2 e .

health information narrowly. The DAA definition would not cover, for example, a consumer's visit to an AIDS-education website or use of a diabetes app. In contrast, the NAI Code defines sensitive health information more broadly as "information, including inferences, about sensitive health or medical conditions, or treatments." Staff encourages both self-regulatory organizations to provide heightened levels of protection for sensitive information, consistent with the Commission's longstanding principles.

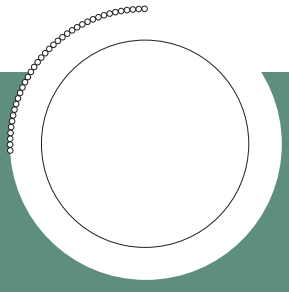
Security

Finally, the FTC Act requires companies to maintain reasonable security, in order to avoid future unexpected and unauthorized uses of data, including by hackers and other wrongdoers who could access the data via a data breach. To this end, companies should keep only the data necessary for their business purposes and properly secure the data they do collect and maintain.[87] As noted above, hackers and others are increasingly targeting the type of rich data sets that cross-device tracking companies collect, which is often tied to individually identifiable information, such as email address or username. Staff commends the DAA and NAI for including the important principle of reasonable security in their codes.

IV. Conclusion

While cross-device tracking provides benefits to consumers and industry, it is important that consumers are informed and able to control tracking that occurs across their devices. FTC staff recommends that those entities with direct consumer-facing relationships and those engaging in cross-device tracking be transparent about their data collection and use practices; improve choice mechanisms to provide consumers control over their data; provide heightened protections for sensitive data; and maintain reasonable security.

[87] *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY &SECURITY IN A CONNECTED WORLD 33–39 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (calling for data minimization and security). Commissioner Ohlhausen dissented from the report's recommendation for data minimization. *See* Separate Statement of Commissioner Maureen K. Ohlhausen Regarding Internet of Things Workshop Report at 2, https://www.ftc.gov/system/files/documents/public_statements/620691/150127iotmkostmt.pdf (criticizing the data minimization recommendation for reflecting a "precautionary principle" approach).



Federal Trade Commission
ftc.gov