CROSS-DEVICE TRACKING

AN FTC STAFF REPORT

Federal Trade Commission
January 2017

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 worked to keep pace with new technological developments in this area, from the use of cookies to track consumers' browsing behavior, to the use of non-cookie technologies, to cross-app tracking, and now, to the tracking of consumers across their numerous devices. The FTC's workshop on cross-device tracking is part of a series of efforts to explore emerging issues in the area of online behavioral advertising.

Cross-device tracking occurs when platforms, publishers, and ad tech companies try to connect a consumer's activity across her smartphones, tablets, desktop computers, and other connected devices. The goal of cross-device tracking is to enable companies to link a consumer's behavior across her devices.

Cross-device tracking serves several purposes. It can enable consumers to log into their email or social media accounts from multiple devices and have a seamless experience. It can also allow consumers to "maintain state," so they can pick up where they left off in a book or movie that they were viewing on a different device. Cross-device tracking also facilitates companies' efforts to prevent fraud, as they learn which devices typically access consumers' accounts.[1] For instance, if there is an unrecognized device, a company can take steps—such as sending an authentication code to an email address or phone number—to ensure that the new device belongs to the consumer who is trying to access an existing account. Finally, companies can analyze an individual consumer's activities based not only on her habits on one browser or device, but on her entire "device graph"—the map of devices that are linked to her, her household, or her other devices. Often, companies combine the information from a consumer's device graph with offline behavior, such as purchases at brick-and-mortar stores.[2] Companies then can use this data for analytics or personalized advertising. Cross-device tracking is most easily performed by

---

[1] *See* Comment #65 from Scott Talbott, Elec. Transactions Ass'n, to Fed. Trade Comm'n 2 (Dec. 16, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/12/00065-99852.pdf; Comment #57 from Jules Polonetsky, Future of Privacy Forum, to Fed. Trade Comm'n, attached report entitled, CROSS DEVICE: UNDERSTANDING THE STATE OF STATE MANAGEMENT 13 (Oct. 16, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00057-98264.pdf.

[2] Transcript of Cross-Device Tracking: An FTC Workshop, in Washington, D.C. (Nov. 16, 2015), Part 1 at 3–4 (Chairwoman Edith Ramirez) [hereinafter XDT Tr. Part 1], https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-1/ftc_cross-device_tracking_workshop_-_transcript_segment_1.pdf; Jessica Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, Beyond Cookies: Privacy Lessons for Online Advertising, at AdExchanger Industry Preview (Jan. 21, 2015), at 2 [hereinafter Beyond Cookies], https://www.ftc.gov/system/files/documents/public_statements/620061/150121beyondcookies.pdf. *See, e.g.*, Allison Schiff, *LiveRamp's On a Quest for the Unified Customer ID—and It's Adding Probabilistic Data Matching as One Option to Get There*, ADEXCHANGER (Nov. 12, 2015), http://adexchanger.com/data-exchanges/liveramps-on-a-quest-for-the-unified-customer-id-and-its-using-probabilistic-data-to-get-there/ (discussing one entity's effort to bring "offline data into the digital environment").

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-device tracking. Specifically, the report recommends that companies engaged in cross-device tracking: (1) be transparent about their data collection and use practices; (2) provide choice mechanisms that give consumers control over their data; (3) provide heightened protections for sensitive information, including health, financial, and children's information; and (4) maintain reasonable security of collected data.

[3] *See* COAL. FOR INNOVATIVE MEDIA MEASUREMENT, BEST PRACTICES IN CROSS-DEVICE AND CROSS-CHANNEL IDENTITY MEASUREMENT 7 (2016) [hereinafter BEST PRACTICES REPORT], http://cimm-us.org/wp-content/uploads/2012/07/CIMM_Best-Practices-in-Cross-Device-and-Cross-Channel-Identity-Measurement.pdf.

[4] *Cf.* DATAXU, UNDERSTANDING TODAY'S CROSS-DEVICE CONSUMER: UNLOCKING THE POWER OF DATA SCIENCE & ANALYTICS TO ENGAGE PEOPLE, NOT DEVICES 5 (2016) [hereinafter CROSS-DEVICE CONSUMER], http://go.dataxu.com/t9Lm1Y0EQc0zh00FM80004a (discussing advertisers' increasing ability to track users across devices).

I. Background

The Commission's 2015 Cross-Device Tracking Workshop focused on a recent trend in behavioral advertising—the ability to link consumers' behavior across devices—and built on the Commission's prior work in this area. Most significantly, in 2009, following a public workshop and public comment period, the FTC staff released a report on behavioral advertising.[5] The report discussed the benefits of the practice, as well as privacy concerns, including the invisibility of data collection, and the risk that information collected—including sensitive information regarding health, finances, or children—could fall into the wrong hands or be used for unanticipated purposes. To address these concerns, FTC staff encouraged industry to provide consumers with basic privacy protections, including transparency and consumer control, reasonable security and limited retention for consumer data, and affirmative express consent for the use of sensitive data.

In response to the Commission's efforts, industry strengthened its self-regulatory regimes and launched initiatives to raise awareness among its members. Notably, the Network Advertising Initiative ("NAI"), an organization of network advertisers formed in 2000, announced a new self-regulatory code requiring transparency, opt-out choice for behavioral advertising, opt-in choice before use of sensitive information for behavioral advertising, and reasonable security.[6] A new trade association called the Digital Advertising Alliance ("DAA") also emerged, and similarly requires companies to inform consumers of data practices, allow consumers to opt out of behavioral advertising, maintain reasonable security for the data collected, and refrain from using sensitive information for behavioral advertising without consumers' opt-in consent.[7]

When FTC staff issued its behavioral advertising report in 2009, the main technology that online advertising companies used to track consumers online was the cookie. Typically, cookies tracked consumers' activities across a single browser. Since 2009, new forms of tracking have emerged, such as tracking through Flash cookies and browser history sniffing. And tracking is no longer limited to websites. A whole mobile ad tracking industry now exists, with companies tracking consumer behavior across mobile apps. Moreover, tracking is not just limited to the online environment. In its data broker report, the FTC discussed the practice of "onboarding," where companies combine offline and online

---

[5] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[6] *See* Press Release, Fed. Trade Comm'n, Federal Trade Commission Issues Report on Online Profiling (July 27, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/federal-trade-commission-issues-report-online-profiling (applauding the NAI for developing a self-regulatory proposal addressing the privacy concerns consumers have about online profiling).

[7] *See* DIGITAL ADVERT. ALL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 12, 14–15, 17 (2009), http://digitaladvertisingalliance.org/sites/digital.daaoperations.org/files/DAA_files/seven-principles-07-01-09.pdf. On the issue of sensitive information, FTC staff has previously noted that the DAA definition of sensitive information is unduly narrow. For example, "health information" is defined to include only medical records or prescriptions. Staff has urged the DAA to expand this definition to be more consistent with NAI's definition. Beyond Cookies, *supra* note 2, at 9–10.

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 devices consumers use grows, so does the potential extent of cross-device tracking.

To engage in cross-device tracking, companies use a mixture of both "deterministic" and "probabilistic" techniques.[12] Generally, deterministic techniques track consumers across devices through a consumer-

---

[8] *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 27–30 (2014) [hereinafter DATA BROKER REPORT], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[9] CROSS-DEVICE CONSUMER, *supra* note 4, at 1.

[10] *See* BEST PRACTICES REPORT, *supra* note 3, at 5 (discussing how "[t]racking consumers across multiple platforms and Internet-connected digital devices (including smart TVs), linking offline and online behavior for the same household or individual via links between home mailing, IP, and e-mail addresses, mobile phone numbers, landlines, device IDs, and cookies now appears to be a mandatory practice for constructing and executing advertising strategies.").

[11] *See* CROSS-DEVICE CONSUMER, *supra* note 4, at 5 (discussing benefits advertisers get from cross-device technology).

[12] *See* CROSS-DEVICE CONSUMER, *supra* note 4, at 6.

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-party advertising

---

[13] CROSS-DEVICE CONSUMER, *supra* note 4, at 6; XDT Tr. Part 1 at 9 (Justin Brookman).

[14] CROSS-DEVICE CONSUMER, *supra* note 4, at 6; XDT Tr. Part 1 at 10 (Justin Brookman).

[15] XDT Tr. Part 1 at 10 (Justin Brookman). *See* CROSS-DEVICE CONSUMER, *supra* note 4, at 6.

[16] *See* XDT Tr. Part 1 at 9 (Justin Brookman); Future of Privacy Forum #57, *supra* note 1, attached report entitled, CROSS DEVICE: UNDERSTANDING THE STATE OF STATE MANAGEMENT at 9–11.

[17] BEST PRACTICES REPORT, *supra* note 3, at 15 (noting IP address is one of the most commonly used data points utilized in consumer matching across devices and platforms).

[18] *See* XDT Tr. Part 1 at 9 (Justin Brookman).

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 are being used by the same consumer. In addition, the ad network may use probabilistic techniques to gain greater certainty of the match and further insights into who the consumer is and how to best target him.[21]

In preparation for the workshop, FTC staff conducted research relating to cross-device tracking.[22] Staff tested 100 popular websites on two devices and made the following findings. First, companies known to engage in cross-device tracking were embedded in at least 87 of the 100 websites.[23] Second, 861 third parties, including those known to engage in cross-device tracking, were observed connecting to both devices. Third, 96 of the 100 websites allowed consumers to submit a username or email address to the site. A first party that collects such a username or email address could share this information with third parties for several reasons, including as described above, to correlate users across devices. Additionally,

---

[19] *See* XDT Tr. Part 1 at 9 (Justin Brookman); *see also* Future of Privacy Forum #57, *supra* note 1, attached report entitled, CROSS DEVICE: UNDERSTANDING THE STATE OF STATE MANAGEMENT at 11.

[20] Hashing refers to the process of transforming a string of characters into another fixed value based on a formula. A hashed email address is one that has been transformed by a mathematical function. In hashed form, the email address is transformed into a sequence of random-looking characters and is not recognizable as an email address, but any time the email address is transformed by a particular hash function, it generates the same hashed value.

[21] *See* BEST PRACTICES REPORT, *supra* note 3, at 9 (discussing how a company that provides one service relying on deterministic data also leverages probabilistic matches for clients who want more information. And another probabilistic company "leverages a small core of deterministic data . . . to train its probabilistic device graph.").

[22] Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, PROC. ON PRIVACY ENHANCING TECH. 113, 117–22 (2017) [hereinafter CROSS-DEVICE TRACKING STUDY], https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.

[23] These companies purport to be dedicated cross-device tracking companies in their advertisements, marketing materials, and public statements. *See, e.g.*, Brian Barrett, *Uh Oh: Google Expands its Ad Tracking. But, Yay: It's Opt-in*, WIRED (June 28, 2016), https://www.wired.com/2016/06/latest-ad-tracking-move-google-gets-opt-right/; *The Largest Independent Cross-Device Identity Solution*, DRAWBRIDGE, https://drawbridge.com/c/graph (last visited Dec. 27, 2016); *What Information Does Facebook Get When I Visit a Site with the Like Button?*, FACEBOOK, https://www.facebook.com/help/186325668085084?sr=1 (last visited Dec. 27, 2016); *Who We Are*, TAPAD, http://www.tapad.com/about-us/who-we-are/ (last visited Dec. 27, 2016).

16 of the 100 websites tested shared username or email (raw or hashed) with third parties.[24] These findings, taken together, suggest that cross-device tracking is common. Consistent with staff's findings, the growth in cross-device tracking has been widely reported.[25] Indeed, an increasing number of companies have advertised cross-device tracking services.[26]

Benefits and Challenges

Like the ability to link consumers across webpages, the ability of businesses to link consumers across different devices creates both benefits and challenges for consumers. One benefit is that cross-device tracking creates a seamless experience for consumers across their devices, such as when they check email, read a book, or watch a movie.

A second benefit is improved fraud detection and account security.[27] As more transactions move online, companies can determine if a consumer is using a new device to access an account and conduct additional authentication to ensure the account belongs to the consumer and not an impostor. Financial institutions in particular often use this technique, which can reduce waste and fraud, and lower the likelihood of identity theft.[28]

Third, cross-device tracking may enable marketers to provide consumers with a better online experience.[29] Consumers may be frustrated if one particular advertisement targets them many times.[30]

---

[24] FTC staff used OpenWPM, an open source web-privacy measurement platform, to observe and analyze the traffic between the websites and third parties. Staff notes that the websites may have engaged in additional sharing that staff could not observe, and there may have been additional email hashes that staff could not confirm.

[25] *See, e.g.*, Letter from Senator Edward J. Markey, Comm. on Commerce, Sci., and Transp., to the Honorable Edith Ramirez, Chairwoman, Fed. Trade Comm'n. (Oct. 10, 2013) , https://static01.nyt.com/packages/pdf/technology/Letter-Cross-Platform-Tracking-FTC.pdf; Claire Cain Miller & Somini Sengupta, *Selling Secrets of Phone Users to Advertisers*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html; Allison Schiff, *2016 Edition: A Marketer's Guide To Cross-Device Identity*, ADEXCHANGER (Feb. 29, 2016), http://adexchanger.com/data-exchanges/2016-edition-marketers-guide-cross-device-identity/.

[26] *See* Comment #61 from Jeff Chester, Ctr. for Dig. Democracy, to Fed. Trade Comm'n 1 (Nov. 16, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/11/00061-99851.pdf; CROSS-DEVICE CONSUMER, *supra* note 4, at 5–6.

[27] *See* Future of Privacy Forum #57, *supra* note 1, attached report entitled, CROSS DEVICE: UNDERSTANDING THE STATE OF STATE MANAGEMENT at 13; Elec. Transactions Ass'n #65, *supra* note 1, at 2.

[28] *See* Elec. Transactions Ass'n #65, *supra* note 1, at 2.

[29] *See, e.g.*, Comment #64 from David Fall, Tapad, Inc., to Fed. Trade Comm'n 1–2 (Dec. 14, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/12/00064-99853.pdf; Comment #54 from Michael Zaneis, Interactive Advert. Bureau, to Fed. Trade Comm'n 2 (Oct. 16, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00054-98261.pdf.

[30] XDT Tr. Part 1 at 17 (Jurgen J. Van Staden).

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

---

[31] CROSS-DEVICE CONSUMER, *supra* note 4, at 5.

[32] *See* Interactive Advert. Bureau #54, *supra* note 29, at 2; Tapad, Inc. #64, *supra* note 29, at 1–2.

[33] CROSS-DEVICE CONSUMER, *supra* note 4, at 5.

[34] XDT Tr. Part 1 at 17 (Jurgen J. Van Staden); BEST PRACTICES REPORT, *supra* note 3, at 8 ("Although first-party data providers, such as Google, Facebook, and Amazon, have scalable log-in data from their massive user bases, they are not always good about sharing such data or they may be restricted in their ability to share data because of privacy policies or contractual commitments, resulting in virtual 'walled gardens' when it comes to identifying users across screens.").

[35] *See New Data: Publishers Look to Harness Real-Time, People-Based Marketing to Compete with Walled Gardens*, MARKET WIRED (Oct. 6, 2015), http://www.marketwired.com/press-release/new-data-publishers-look-harness-real-time-people-based-marketing-compete-with-walled-2061424.htm. *See, e.g.*, CROSS-DEVICE CONSUMER, *supra* note 4, at 10 ("Rather than restricting an advertiser to a specific data provider, DataXu leverages a blend of third-party and in-house data to provide a choice of targeting settings that toggle between scale and accuracy.").

[36] *See, e.g.*, CROSS-DEVICE CONSUMER, *supra* note 4, at 5.

[37] *See, e.g.*, Tapad, Inc. #64, *supra* note 29, at 2; CROSS-DEVICE CONSUMER, *supra* note 4, at 5. *See also* XDT Tr. Part 1 at 17–19 (Jurgen J. Van Staden).

[38] *See* Comment #69 from Khaliah Barnes, Elec. Privacy Info. Ctr., to Fed. Trade Comm'n 4 (Dec. 16, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/12/00069-99857.pdf.

[39] *Cf.* Blase Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising* 9, SYMPOSIUM ON USABLE PRIVACY & SEC. (2012), https://cups.cs.cmu.edu/soups/2012/proceedings/a4_Ur. *See also* Comment #56 from Chris Calabrese et al., Ctr. for Democracy & Tech., to Fed. Trade Comm'n 8 (Oct. 16, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00056-99849.pdf.

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. Trade Comm'n (Nov. 13, 2015) ("Cross-device technology is an unwelcome invasion on consumer privacy."), https://www.ftc.gov/policy/public-comments/2015/11/13/comment-00059.

[41] *See, e.g.*, Amy Pittman, *The Internet Thinks I'm Still Pregnant*, N.Y. TIMES (Sept. 2, 2016), http://www.nytimes.com/2016/09/04/fashion/modern-love-pregnancy-miscarriage-app-technology.html (noting the author, when downloading and entering information into a pregnancy app, "hadn't realized . . . the company would then share it with marketing groups targeting new mothers." Despite having entered the miscarriage in the app, the author explains, "As far as the internet is concerned, my pregnancy proceeded normally and I gave birth and became a mother last month.").

[42] *See, e.g.*, Marc Groman, *No One Should Be Outed By an Ad*, IAPP, (Feb. 24, 2015), https://iapp.org/news/a/nai-takes-lgbt-stand/ (discussing how "developments in cross-device tracking mean that ads for gay events or venues could surface not only on [a] home computer where [a consumer] originally searched for the information, but on [a] work laptop or tablet. . . . [T]he ads could even be displayed on [the] parents' computers, which could unknowingly be linked to [the consumer's] PC because they appear to be part of the same household.").

[43] *See, e.g.*, Ctr. for Democracy & Tech. #56, *supra* note 39, at 2, 8; Ctr. for Dig. Democracy #61, *supra* note 26, at 3; CROSS-DEVICE CONSUMER, *supra* note 4, at 5; Justin Civello, *Completing the Picture: Offline Attribution*, DRAWBRIDGE (Nov. 24, 2015), https://www.drawbridge.com/blog/p/product-updatenbspcompleting-the-picture-offline-attribution. *See also* DATA BROKER REPORT, *supra* note 8, at 27–30; XDT Tr. Part 1 at 3–4 (Chairwoman Edith Ramirez).

Companies do not appear to be explicitly discussing cross-device tracking practices in their privacy policies. For example, FTC staff's review of privacy policies for one hundred top websites found minimal explicit disclosure to consumers about whether and how cross-device tracking occurs.[44] Of the one hundred privacy policies reviewed, staff found only three policies that explicitly mentioned enabling third-party cross-device tracking on their site.[45]

Not only is the *practice* of cross-device tracking opaque to consumers but so are the myriad entities that have access to, compile, and share data in the tracking ecosystem.[46] While a continuous experience may be intuitive when a consumer logs into the same service on different devices, third-party advertising and analytics companies with which the consumer has no relationship may also track her activity across devices.[47] Similar issues apply to third-party advertising networks in general. And the Commission's Data Brokers report also discussed the dozens of companies that enable data brokers to collect consumers' personal information, most ofwhich have little or no direct consumer interaction.[48]

A second challenge associated with cross-device tracking is that consumers who may be uncomfortable with the practice have only limited choices to control it. Studies show that a large number of consumers currently take steps to limit data collection.[49] Some surveys suggest that 30% to almost 50% of internet users delete their cookies every month.[50] As of January 2016, 29% of consumers in the United States and United Kingdom reported that they had turned on the Limit Ad Tracking setting for their iOS and Android smartphones.[51] In addition, consumers are increasingly turning to ad blockers. One recent study

---

[44] XDT Tr. Part 1 at 13 (Justin Brookman).

[45] CROSS-DEVICE TRACKING STUDY, *supra* note 22.

[46] *See* Transcript of Cross-Device Tracking: An FTC Workshop, in Washington, D.C. (Nov. 16, 2015), Part 2 at 3–4, 8, 16 (Joe Turow, Laura Moy in conversation) [hereinafter XDT Tr. Part 2], https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-2/ftc_cross-device_tracking_workshop_-_transcript_segment_2.pdf.

[47] *Cf.* XDT Tr. Part 2 at 1–2 (Jason Kint) (discussing how consumers can choose to end first-party relationships if they are served ads that surprise them or make them uncomfortable).

[48] *See* DATA BROKER REPORT, *supra* note 8, at 3, 11–15, 46.

[49] Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RESEARCH CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ ("Some 86% of internet users have taken steps to remove or mask their digital footprints, but many say they would like to do more or are unaware of tools they could use.").

[50] COMSCORE, THE IMPACT OF COOKIE DELETION ON SITE-SERVER AND AD-SERVER METRICS IN AUSTRALIA: AN EMPIRICAL COMSCORE STUDY 14 (2011), http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/The_Impact_of_Cookie_Deletion_on_Site-Server_and_Ad-Server_Metrics_in_Australia_An_Empirical_comScore_Study (discussing various findings on consumer cookie deletion).

[51] Kate Kaye, *Use of Limit Ad Tracking Drops as Ad Blocking Grows*, ADVERTISINGAGE, (May 9, 2016), http://adage.com/article/privacy-and-regulation/limit-ad-tracking-drops-ad-blocking-grows/303911/.

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. respondents identified privacy concerns as a reason.[53] Even as consumers have become savvier about making choices to opt out of traditional online tracking, some of these choices may not apply to cross-device tracking.

Finally, there may be security-related concerns when cross-device tracking companies collect and aggregate vast amounts of data about sites visited and apps used, often in conjunction with raw or hashed email addresses.[54] Hackers often target large caches of information, as recently announced breaches demonstrate.[55] Even though cross-device tracking information may not contain credit card or financial account numbers, or Social Security numbers, consumers can be harmed if it is released without authorization.[56] These harms could include the posting of highly-private information on a public website, including health information or other sensitive information gleaned from internet browsing histories. Wrongdoers may also access the information to engage in blackmail[57] or to conduct especially effective spear phishing campaigns.[58] Further, if third-party archives of consumer information are breached, other security measures such as knowledge-based authentication could become less effective.

---

[52] PAGEFAIR, ADBLOCKING GOES MOBILE: PAGEFAIR 2016 MOBILE ADBLOCKING REPORT 4 (2016) https://pagefair.com/downloads/2016/05/Adblocking-Goes-Mobile.pdf.

[53] HUBSPOT RESEARCH, WHY PEOPLE BLOCK ADS: AND WHAT IT MEANS FOR MARKETERS AND ADVERTISERS 8 (2016), https://research.hubspot.com/reports/why-people-block-ads-and-what-it-means-for-marketers-and-advertisers.

[54] *See, e.g.*, Ctr. for Democracy & Tech. #56, *supra* note 39, at 9; Elec. Privacy Info. Ctr. #69, *supra* note 38, at 4.

[55] *Cf.*, Ruby Corp., Ruby Life Inc., 152 3284 (F.T.C Dec. 14, 2016) (complaint) https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf; Brian Krebs, *Was the Ashley Madison Database Leaked?*, KREBS ON SEC. (Aug. 18, 2015), http://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/; Roi Perez, *Dropbox Hack Confirmed Real*, SC MAGAZINE (Aug. 31, 2016), http://www.scmagazineuk.com/dropbox-hack-confirmed-real-68-million-accounts-affected/article/519545/; Brian Krebs, *Data Breach at Health Insurer Anthem Could Impact Millions*, KREBS ON SEC. (Feb. 4, 2015), http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/.

[56] *Cf.* Christopher Mims, *The Hacked Data Broker? Be Very Afraid*, WALL ST. J. (Sept. 8, 2015), http://www.wsj.com/articles/the-hacked-data-broker-be-very-afraid-1441684860.

[57] *Cf.* Alex Hern, *Spouses of Ashley Madison Users Targeted with Blackmail Letters*, THE GUARDIAN (Mar. 3, 2016), https://www.theguardian.com/technology/2016/mar/03/ashley-madison-users-spouses-targeted-by-blackmailers.

[58] Spear phishing occurs when consumers receive emails from fraudsters that look legitimate (as though from reputable businesses) and contain personal details, tricking the consumer into clicking on a link, which then compromises a computer. *See Spear Phishing: Scam, Not Sport*, NORTON, https://us.norton.com/spear-phishing-scam-not-sport/article (last visited Dec. 27, 2016); *Consumer Information: Phishing*, FED. TRADE COMM'N (Sept. 2011), https://www.consumer.ftc.gov/articles/0003-phishing; Mims, *supra* note 56.

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/2134006/data-protection/hack-of-major-data-brokers-weakens-bank-authentication.html; Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?_r=0 (noting potential exposure of answers to security questions).

[60] NETWORK ADVERT. INITIATIVE, GUIDANCE FOR NAI MEMBERS: USE OF NON-COOKIE TECHNOLOGIES FOR INTEREST-BASED ADVERTISING CONSISTENT WITH THE NAI CODE OF CONDUCT 2 (2015) [hereinafter GUIDANCE FOR NAI MEMBERS], http://www.networkadvertising.org/sites/default/files/NAI_BeyondCookies_NL.pdf.

[61] *Id*. at 2.

[62] *Id*. at 3.

[63] *Id*. at 2 & n.4.

[64] Press Release, ASRC, "Cookie-less" Technologies Subject to Accountability Program Enforcement (Aug. 21, 2014), http://www.bbb.org/council/news-events/news-releases/2014/08/cookie-less-technologies-subject-to-accountability-program-enforcement.

[65] DIG. ADVERT. ALL., APPLICATION OF THE SELF-REGULATORY PRINCIPLES OF TRANSPARENCY AND CONTROL TO DATA USED ACROSS DEVICES 2 (2015) [hereinafter DAA CROSS-DEVICE GUIDANCE], http://www.aboutads.info/DAA_Cross-Device_Guidance-Final.pdf.

cannot be used for behavioral advertising on other devices.[66] Similarly, data collected from other devices cannot inform ads on the opted-out device.[67] DAA has stated it will begin enforcing this application of its Principles in February 2017.[68]

FTC staff commends these self-regulatory efforts to improve transparency and choice in the cross-device tracking space. Both the NAI and DAA have taken steps to keep up with evolving technologies and provide important guidance to their members and the public. Their work has improved the level of consumer protection in the marketplace. However, both organizations could strengthen their efforts to address cross-device tracking, as described further below.[69]

III. Recommendations

This section of the report is intended to encourage publishers, companies engaged in cross-device tracking, and self-regulatory organizations to address the concerns about transparency, choice, sensitive data, and security raised at the workshop. It explains how these basic principles can be adapted to the new realm of cross-device tracking and describes some lessons learned from relevant FTC enforcement actions.

Transparency

Consistent with longstanding FTC principles,[70] all companies engaged in cross-device tracking—both the companies themselves and publishers who hire these companies—should truthfully disclose their

---

[66] *Id*. at 4.

[67] *Id*.

[68] Press Release, Dig. Advert. All., Digital Advertising Alliance Announces Enforcement of Cross-Device Guidance to Begin February 1, 2017 (Oct. 13, 2016), http://www.aboutads.info/digital-advertising-alliance-announces-enforcement-cross-device-guidance-begin-february-1-2017.

[69] For example, FTC staff encourages self-regulatory organizations to make clear the effective dates of their principles and codes, as well as the scope of their application. The NAI and DAA have multiple sets of codes, principles, and guidance, some of which are best practices and some of which are enforced. For example, the NAI announced its guidance on non-cookie technologies in May 2015 but does not yet enforce it, and the DAA stated it would begin enforcing its November 2015 cross-device guidance in February 2017. In addition, it is not apparent to us whether the NAI's Code of Conduct, which applies to "data collected across web domains," covers browsing behavior on smart televisions. Staff encourages more clarity on both of these points so that companies and consumers know the standards to which self-regulatory organizations hold their members.

[70] *See, e.g.*, FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007), https://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf (statement of the Bureau of Consumer Protection proposing governing principles for online behavioral advertising and requesting comment). Self-regulatory organizations have also advocated for transparency. *See, e.g.*, NETWORK ADVERT. INITIATIVE, 2008 NAI

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 audio beacons in their apps, through software called Silverpush, without informing consumers who downloaded the apps.[72] The software was capable of listening to a television being played near the consumer's mobile device, and producing a detailed log of the television content viewed, for the purpose of targeted advertising and analytics. Staff warned these developers that, if "your application enabled third parties to monitor television-viewing habits of U.S. consumers and your statements or user interface stated or implied otherwise, this could constitute a violation of the Federal Trade Commission Act."[73] And as companies develop internet of things devices (such as smart televisions) that track consumers, it is important that these companies also explain to consumers what information is collected from the device, the entities that are collecting information, and how they use and share the information collected.

Another aspect of transparency is making truthful claims about the categories of data collected. Often, raw email addresses and usernames are personally identifiable, in that they include full names. Even hashed email addresses and usernames are persistent identifiers and can be vulnerable to reidentification in some cases.[74] The Commission has repeatedly stated that data that is reasonably linkable to a

---

PRINCIPLES 7 (2008) http://www.networkadvertising.org/sites/default/files/imce/2008_principles.pdf; DIG. ADVERT. ALL., *supra* note 7, at 12–13.

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

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

[73] *Id*. (including a link to the warning letters).

[74] *See supra* note 20. For example, if a hacker were able to access a cache of hashed email addresses exposed by a data breach, it would be relatively easy, in many instances, for the hacker to determine the original email addresses. The hacker

consumer or a consumer's device is personally identifiable.[75] Therefore, consumer-facing companies that provide raw or hashed email addresses or usernames to cross-device tracking companies should refrain from referring to this data as anonymous or aggregate, and should be careful about making blanket statements to consumers stating that they do not share "personal information" with third parties.[76]

The Commission's case against MySpace is instructive in this regard.[77] MySpace told consumers that it did not share personal information with third parties. It did, however, share a "FriendID" with advertisers that enabled the advertisers to take simple steps to access consumers' personal information. The Commission alleged that this practice was deceptive, in violation of the FTC Act.

Choice

As with traditional forms of tracking, companies should offer consumers choices about how their cross-device activity is tracked. And, when companies offer such choices, the FTC Act requires that the companies respect them. To the extent opt-out tools are provided, any material limitations on how they apply or are implemented with respect to cross-device tracking must be clearly and conspicuously disclosed. The Commission's case against the online advertising company ScanScout is instructive

---

could use the same hash function to hash thousands of email addresses, and look for matches among the cache. Experts have advised "salting" data, which refers to adding data to a data set before hashing it, to add some protection by defending against such attacks, but it is not a substitute for implementing a broader security program. *See* XDT Tr. Part 1 at 24–25 (Jonathan Mayer).

[75] *See infra* note 76. *See also* Comment of the Staff of the Bureau of Consumer Protection to the Fed. Commc'n Comm'n at 9-10 (May 27, 2016), https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/05/comment-staff-bureau-consumer-protection-federal.

[76] As discussed in the Commission's 2012 report, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, the Commission considers data that can be reasonably linked to a specific consumer, computer, or other device to be personal information. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 22 (2012) [hereinafter PRIVACY REPORT], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Further to this point, the Children's Online Privacy Protection Act ("COPPA") defines "personal information" to include persistent identifiers that can be used to recognize a user over time and across different websites or online services, such as a cookie, IP address, serial number, or unique device identifier. 15 U.S.C. § 6501(8) (1998); 16 C.F.R. § 312.2(7) (2013). However, certain obligations under COPPA, such as notice of information collection and parental consent, do not apply when personal information is used in support of internal operations of a website or online service, including maintaining or analyzing the function of the website or service (*e.g.* for functionality, network communications, security, etc.). COPPA, 15 U.S.C. §§ 6501–6506; Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013) (implementing enhanced protections for children's information).

Commissioner Ohlhausen notes that to the extent that an email address is hashed in a manner so that it is not reasonably linkable to a consumer or a consumer's devices, it would not be personally identifiable information under the FTC's long-standing principles.

[77] MySpace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) (complaint) https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacecmpt.pdf.

about the importance of communicating the limitations of an opt-out. In that case, the Commission alleged that the company violated Section 5 of the FTC Act when it told consumers that they could opt out of tracking by using their browser-based opt-out tools but, in fact, the company continued to track consumers using Flash cookies.[78] Any browser-based opt-out would have been ineffective in stopping tracking through Flash cookies.

Similarly, in the Commission's recently announced settlement with Turn, an online advertising company, the Commission alleged that the company continued to target ads to consumers through an identifier, despite representing that consumers could opt out of interest-based advertising by instructing their browser to stop accepting cookies.[79] These cases send an important message: If a company offers an opt-out that is limited to only certain types of tracking technologies, the company must clearly and conspicuously disclose the limits of the opt-out to avoid misleading consumers.[80]

In order to ensure that all actors in the ecosystem are making truthful claims about the choices afforded to consumers, consumer-facing companies that utilize third-party companies for cross-device tracking—and the cross-device tracking companies themselves—should coordinate efforts. For example, app developers frequently embed software code of third-party ad networks—known as ad libraries—into their apps in order to display ads within their apps and generate advertising revenue.[81] Behind-the-scenes third-party tracking companies may themselves be subject to liability when they misrepresent to app developers the types of information they collect and use, as happened in the Commission's recent case against mobile ad network InMobi.[82] There, the Commission alleged that InMobi misrepresented to its app developer customers that its advertising software would track consumers' locations only when they opted in through their devices' privacy settings. However, the FTC alleged InMobi's software tracked consumers' location even if they denied permission. The Commission alleged that InMobi's misrepresentations to app developers were deceptive in violation of Section 5 of the FTC Act.

As with transparency, the self-regulatory organizations NAI and DAA have done important work on educating companies about the need to provide choices to consumers with respect to cross-device tracking, including by issuing new guidance related to this practice. As noted above, starting in February 2017, the DAA will require that a consumer's opt-out on one device to prevent that device from

---

[78] ScanScout, Inc., No. C-4344 (F.T.C. Dec. 14, 2011) (complaint) https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutcmpt.pdf.

[79] Turn Inc., No. 152 3099 (F.T.C. Dec. 20, 2016) (complaint) https://www.ftc.gov/system/files/documents/cases/turn_inc_final_complaint.pdf.

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

[81] Andrea Arias, *Ad Libraries and App Developers, Check Out This Advice*, FED. TRADE COMM'N: BUSINESS BLOG (Sept. 16, 2016, 10:44 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/09/ad-libraries-app-developers-check-out-advice.

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

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 that device. Conversely, a company may wrongly associate a device with a consumer who opts out, stop serving ads on that device, and anger the consumer who owns the device and wants to receive targeted ads or services that rely on cross-device tracking. These concerns are valid. As time goes on and tracking techniques improve, however, companies should continue to reassess technical limitations and simplify consumer choices wherever possible.

Sensitive Data

FTC staff also recommends that companies refrain from engaging in cross-device tracking on sensitive topics, including health, financial, and children's information,[85] without consumers' affirmative express consent. Staff further recommends that they refrain from collecting and sharing precise geolocation information without consumers' affirmative express consent. The FTC has previously stated that these categories of data are sensitive, warranting higher levels of protection.[86]

The principles and codes of conduct governing the online advertising industry generally recognize the need for heightened consent for sensitive data. For example, the NAI Code requires members to obtain consumers' opt-in consent before using sensitive data or precise location information for interest-based advertising. The DAA Principles similarly require opt-in consent before using consumers' sensitive data or precise geolocation information for interest-based advertising, but DAA defines sensitive data as to

---

[83] DAA CROSS-DEVICE GUIDANCE, *supra* note 65, at 4; Dig. Advert. All., *supra* note 68.

[84] Commissioner Ohlhausen notes that even if a single opt-out were easy to effectuate, some consumers may still prefer the flexibility of a device-by-device opt-out. In her view, companies should explore many alternatives to offering consumers choice.

[85] Child-directed websites and apps may have additional obligations under COPPA, 15 U.S.C. §§ 6501–6506 (1998); Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013).

[86] *See* PRIVACY REPORT, *supra* note 76, at 58–60; In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, F.C.C. WC DOCKET NO. 16-106, at 21–23 (F.C.C. filed May 27, 2016), (Fed. Trade Comm'n staff comment), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

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