epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Comments of

THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE FEDERAL TRADE COMMISSION,

Cross-Device Tracking Workshop

December 16, 2015

By notice published on October 16, 2015, the Federal Trade Commission ("FTC" or "Commission") seeks public comments on the privacy implications of "cross-device tracking."[1] Cross-device tracking is the "tracking of consumers' activities across their different devices for advertising and marketing purposes."[2] The FTC hosted a workshop on November 16, 2015 to explore cross-device tracking privacy issues.[3] Following the FTC's examination of cross-device tracking, the Commission should now take affirmative steps to protect consumer privacy in light of the substantial privacy risks identified during the workshop. Specifically, the FTC should: (1) issue regulations on cross-device tracking privacy protections based on the Consumer Privacy

[1] Federal Trade Commission, Notice of Workshop and Opportunity for Comment (Oct. 16, 2015), https://ftcpublic.commentworks.com/ftc/crossdeviceWorkshop/.
[2] *Id*.
[3] Federal Trade Commission, Cross-Device Tracking (Nov. 16, 2015), https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

Bill of Rights, not an ineffective "notice and choice" system; (2) update the Children Online Privacy Protection Act ("COPPA") regulations to reflect cross-device tracking practices that affect minors; and (3) use its Section 5 enforcement authority to prevent deceptive cross-device tracking practices.

EPIC's Interest

The Electronic Privacy Information Center ("EPIC") is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and related human rights issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[4] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and subsequent October 24, 2011 settlement concerning the improper disclosure of user information.[5] The Commission's settlement with Facebook followed from a complaint filed by EPIC and a coalition of privacy and civil liberties organizations in December 2009 and a Supplemental Complaint filed by EPIC in February 2010.[6]

---

[4] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[5] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").

[6] Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [hereinafter EPIC 2009 Facebook Complaint]; Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and

EPIC has also submitted comments for and participated in several Commission workshops, such as Face Facts: A Forum on Facial Recognition Technology,[7] and In Short: Advertising and Privacy Disclosures in a Digital World.[8] EPIC has also defended the FTC in its recent dispute with Wyndham Hotels regarding the FTC's ability to enforce data security standards.[9]

More recently, EPIC has urged the Commission to protect consumer privacy amid emerging technology, including the "Internet of Things,"[10] and "always on" consumer devices.[11] The Commission, however, has failed to take action despite the inherent and increasing privacy and security risks associated with connected devices and other emerging technology.[12] The FTC's failure to promptly investigate business practices, pursue complaints, or modify proposed settlements to reflect public comments it has explicitly requested is (1) contrary to the explicit purpose of the statutory provision that allows the Commission to request comments from the

---

Request for Injunction, Request for Investigation and for Other Relief) [hereinafter EPIC 2009 Facebook Supplement]; Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [hereinafter EPIC 2010 Facebook Complaint].

[7] Face Facts: A Forum on Facial Recognition Technology, Fed. Trade Comm'n, http://www.ftc.gov/bcp/Workshops/facefacts/ (last visited Dec. 16, 2015).

[8] In Short: Advertising and Privacy Disclosures in a Digital World, Fed. Trade Comm'n, https://www.ftc.gov/news-events/events-calendar/2012/05/short-advertising-privacy-disclosures-digital-world (last visited Dec. 16, 2015).

[9] *See* Amicus Curiae Brief of Electronic Privacy Information Center (EPIC), *FTC v. Wyndham Worldwide Corp*., No. 14-3514 (3rd Cir. Nov. 12, 2014), *available at* https://epic.org/amicus/ftc/wyndham/Wyndham-Amicus-EPIC.pdf.

[10] EPIC, On the Privacy and Security Implications of the Internet of Things (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.

[11] *See, e.g.*, In the Matter of Samsung Electronics Co., Inc., (2015) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.; Letter from EPIC to U.S. Dep't of Justice, Fed. Trade Comm'n Re: "Always On" Consumer Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.

[12] Letter from EPIC to Rep. Darrell Issa, Chairman, Comm. on Oversight and Gov't Reform Re: "The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury" (July 25, 2014) https://epic.org/privacy/ftc/EPIC-Congress-re-FTC.pdf.

public;[13] (2) contrary to the broader purpose of the Commission to police unfair and deceptive trade practices;[14] and (3) contrary to the interests of American consumers.

EPIC offers these recommendations to protect the interests of consumers and to urge the FTC to take meaningful action on this and other issues that EPIC has recently brought to the Commission's attention.

I. Cross-Device Tracking Lacks Transparency and Control, While Collecting Increasingly Sensitive, Personal, and Comprehensive Information About Consumers

The FTC Cross-Device Tracking Workshop (the "Workshop") provided a useful analysis of various cross-device tracking techniques and identified numerous privacy challenges to consumers, particularly the lack of transparency and control in this undetectable online tracking scheme.

One clear message from the FTC's Cross-Device Tracking Workshop is that consumers lack meaningful control over this intrusive business practice. At the Workshop, the FTC's Office of Technology, Research, and Investigation Policy Director Justin Brookman admitted that it's "really hard to determine objectively, from the end user point of view, when cross device tracking is going on."[15] The average consumer – with no expectation or indication that such complex profiling is taking place – should not bear the burden of detecting these surreptitious practices.

Compounding the secrecy of these practices, companies that engage in cross-device tracking collect vast amounts of personal, sensitive information. As many of the Workshop

[13] Commission Rules of Practice, 16 C.F.R. § 2.34 (C) (2014).
[14] Federal Trade Commission Act, 15 U.S.C. § 46 (2006).
[15] *See* Fed'l Trade Comm'n Workshop Transcript Segment 1: Cross-Device Tracking 13 (Nov. 16, 2015), *available at* https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-1/ftc_cross-device_tracking_workshop_-_transcript_segment_1.pdf [hereinafter Workshop Transcript Segment 1].

panelists recognize, tracking consumer behavior across numerous connected devices creates detailed consumer profiles. As this practice becomes more widespread, the risks to consumer privacy will increase.

First, connected devices such as smartphones and wearable health devices produce sensitive data not typically available from traditional computer web browsing. For example, smartphones enable comprehensive location tracking that can reveal a person's social, professional, and personal identity.[16] Many smartphones also contain sensors, such as barometers, accelerometers, and altimeters.[17]

Second, while data may not be considered sensitive or personal on one device, it may become highly sensitive or personal when combined with data from linked devices. For example, as Chairwoman Edith Ramirez suggested at the Workshop, "someone who searches online about a medical condition in the privacy of her home could very well see advertisements the next day at work related to that condition or the next evening on the families smart TV."[18] An employee who is job hunting from her tablet at home may later be shown job search ads on her work computer.

Furthermore, both deterministic and probabilistic cross-device tracking rely on personal information. Deterministic, login-based tracking directly relies on personally identifiable information, which necessarily implicates privacy interests. As described by an online advertising trade publication,

---

[16] *See* Amicus Curiae Brief of Electronic Privacy Information Center (EPIC), In re: Application of the United States of America for Historic Cell Site Data, No. 20884 (5th Cir. Mar. 16, 2012), available at https://epic.org/amicus/location/cell-phone-tracking/EPIC-5th-Cir-Amicus.pdf.

[17] *See, e.g.*, Dan Nosowitz, *So, Um, Why Does the New Google Phone Have a Barometer in It?*, POPSCI (Oct. 19, 2011), http://www.popsci.com/gadgets/article/2011-10/so-um-why-does-new-google-phone-have-barometer-it.

[18] Workshop Transcript 1 at 2.

> The deterministic method relies on personally identifiable information (PII) to make device matches when a person uses the same email address to log into an app and a website, thereby creating cross-device linkage. As long as a user is logged in across devices, advertisers and publishers can use this unique identifier to target those users on multiple screens with near-perfect precision.[19]

And the data collected via deterministic tracking in available not only to the company operating the login platform but also to third-party partners. Using hashed personally identifiable information to facilitate cross-device tracking does not sufficiently anonymize this data or provide meaningful privacy protections for consumers.[20]

Probabilistic tracking uses aggregated data collected from multiple devices, such as operating system, IP address, locational data, and device specifications, from which companies create a "digital fingerprint" to identify the specific user linked to multiple devices via statistical inferences.[21] The inherent purpose of this tracking mechanism is to identify a specific individual. The data used to make these specific identifications becomes personally identifying information, regardless of whether this data may, on its own, be "anonymous." Iain Bourne with the UK's Information Commissioner's Office, echoed this understanding: "It's not really worth having a long debate about whether this is not personal information when it's aimed at identifying people."[22]

---

[19] Allison Schiff, *A Marketer's Guide to Cross-Device Identity*, AdExchanger (Apr. 9, 2015) http://adexchanger.com/data-exchanges/a-marketers-guide-to-cross-device-identity/.
[20] Ed Felten, *Does Hashing Make Data "Anonymous"?*, Tech@Ftc (Apr. 22, 2012), https://techatftc.wordpress.com/2012/04/22/does-hashing-make-dataanonymous.https://techatftc.wordpress.com/2012/04/22/does-hashing-make-data-anonymous/.
[21] Allison Schiff, *A Marketer's Guide to Cross-Device Identity*, AdExchanger (Apr. 9, 2015) http://adexchanger.com/data-exchanges/a-marketers-guide-to-cross-device-identity/
[22] *Adobe Summit EMEA: Brands Advised To Always Assume It's Personal*, CMO.com (April 29, 2015) http://www.cmo.com/articles/2015/4/29/adobe-summit-emea-brands-advised-to-always-assume-its-personal.html.

II. EPIC Recommendations and Responses to Remaining FTC Workshop Questions

The Workshop posed several questions about how best to address the privacy implications of cross-device tracking. Specifically, questions remained unanswered regarding the amount of transparency and the substance of disclosures that should be given to consumers regarding cross-device tracking. Questions regarding the extent of consumer control over this tracking and the means of exercising that control also remain. Threshold questions, such as whether such data should be collected or retained, were not even considered. EPIC proposes the following recommendations to the FTC to address these and other privacy-related questions raised by cross-device tracking.

A. The FTC Should Issue Regulations for Cross-Device Tracking Privacy Protections Based on the Consumer Protection Bill of Rights, Not "Notice and Choice"

EPIC has previously alerted the FTC to the problems of "notice and choice," an ineffective policy approach that clearly favors the interests of businesses over consumers and fails to establish meaningful privacy safeguards.[23] Contrary to industry representations,[24] notice or "enhanced notice" will not provide meaningful consumer safeguards. Providing vague information about data collection practices cannot replace concrete data protection obligations or privacy enhancing techniques to minimize or eliminate the collection of consumer information.

---

[23] *See* EPIC Comments to the FTC on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Feb. 18, 2011), *available at* https://epic.org/privacy/ftc/EPIC_Comments_FTC_Internet_Privacy_Report.pdf; EPIC Comments to the FTC on Advertising and Privacy Disclosures in a Digital World (May 11, 2012), *available at* https://epic.org/privacy/ftc/EPIC-FTC-Ad-Disclosures-FINAL.pdf.

[24] *See, e.g.*, Fed'l Trade Comm'n Workshop Transcript Segment 2: Cross-Device Tracking 4 (Nov. 16, 2015), *available at* https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-2/ftc_cross-device_tracking_workshop_-_transcript_segment_2.pdf [hereinafter Workshop Transcript Segment 2].

Emphasizing notice or disclosure is an ineffective means of protecting the privacy rights of consumers. Privacy experts and social scientists have identified several important flaws with a notice-centric approach to protecting privacy. Privacy notices must confront what Professor Helen Nissenbaum termed the "transparency paradox," where the clarity of a notice is in tension with its comprehensiveness.[25] Privacy notices also do not address the "take it or leave it" basis on which most companies continue to offer privacy to consumers. Additionally, a host of cognitive and behavioral hurdles limit the effectiveness of even ideal notices. Further, companies routinely change privacy policies, making even the best efforts of consumers to operate within a notice and choice framework a waste of time. Finally, notices and disclosures do not provide any substantive protections for the privacy of consumers. As a result of these flaws, it is hardly surprising that consumers simply do not read privacy notices, privacy policies, or terms of service. Consumers are rational actors and understand that it is nonsensical to click through 100 privacy settings or read policy statements longer than the US Constitution when there is no practical benefit to them. Similarities between mobile advertising and traditional digital contexts suggest that an approach that emphasizes notice for mobile advertisements will suffer from the same flaws. Indeed, to the extent that the mobile context is unique, its unique features only heighten the flaws that privacy disclosures must confront.

On the other hand, in 2012, President Obama announced the Consumer Privacy Bill of Rights ("CPBR").[26] It is a critical policy framework that provides a blueprint for protecting

[25] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140(4) Daedalus 32, 36 (2011) *available at* http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf. *See also* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2011 Stan. Tech. L. Rev. 1 (2001).

[26] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter White House, CPBR]; *see*

privacy in the modern age. Based on Fair Information Practices, the CPBR is a framework that grants consumer rights and places obligations on private companies collecting consumer information:

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Security: Consumers have a right to secure and responsible handling of personal data.
- Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.

In the context of privacy practices specifically for cross-device tracking, the FTC should issue cross-device tracking regulations that, at a minimum, require:

- Companies to obtain opt-in consent from consumers. In light of the surreptitious nature of cross-device tracking and the increasingly sensitive and personal information it collects, placing the burden on consumers to navigate this complex field through an "opt-out" policy is inapposite.
- Companies to adopt privacy enhancing techniques, which minimize or eliminate the collection or maintenance of personally identifiable information.
- Companies to clearly inform consumers if companies engage in cross-device tracking, what information is collected, used, and disclosed for this activity and to whom.
- Companies to permit consumers' access to their information collected across devices and to amend or delete their information.
- Companies to adopt data security standards.

B. The FTC Should Update its COPPA Regulations to Reflect Cross-Device Tracking Practices that Affect Minors

The FTC should amend the COPPA Rule to either (a) prohibit the cross-device tracking of minors or, in the alternative, (b) require companies to obtain verifiable parental consent before

---

also White House Sets Out Consumer Privacy Bill of Rights, EPIC, http://epic.org/2012/02/whitehouse-sets-out-consumer-.html (last visited Dec. 16, 2015).

engaging in cross-device tracking of minors. COPPA requires parental consent before collecting any personal information from a child.[27] As explained above, cross-device tracking necessarily involves "personal information" under COPPA's broad definition.[28]

Furthermore, the FTC should amend the COPPA Rule to clarify that parental consent applies solely to the device through which parental consent was granted and cannot be transferred to any associated devices. To illustrate, if a parent consents to a website collecting information about her child via the family laptop, that website is prohibited from collecting information about the child while she is using a smartphone unless verifiable parental consent is separately obtained for that device as well.

C. The FTC Should Use its Section 5 Enforcement Authority to Prevent Deceptive Cross-Device Tracking Practices

FTC should use its Section 5 enforcement authority to prohibit deceptive privacy disclosures, particularly deception by omission.[29] A company's failure to disclose the use of consumer data for purposes of cross-device tracking is deceptive by omitting material information about the extent of information collected on the consumer and the manner in which it is used. As Chairwoman Ramirez recognized at the Workshop, "consumers lack of awareness of and choices about tracking. As it currently stands, there are almost no tools that allow individuals to know what devices are linked together by tracking companies or specifically linked to them."[30]

[27] *See* 16 C.F.R. § 312.5(c).
[28] *See* 16 C.F.R. § 312.2.
[29] Fed. Trad Comm'n, Policy Statement on Deception (1983), *available at* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf
[30] Workshop Transcript Segment 1 at 4.

The FTC should also bring Section 5 enforcement actions against companies who engage in cross-device tracking but whose privacy policies claim they do not collect personally identifiable information from consumers. As explained above, all data used to engage in cross-device tracking is inherently identifiable because it is used for the express purpose of identifying a specific individual user of specific devices.

III. Conclusion

EPIC supports the FTC's investigation into the privacy implications of cross-device tracking, but the agency must do more. Privacy protections based on industry self-regulation and burdensome "notice and choice" policies do not provide meaningful safeguards for consumers. The FTC must issue effective regulations and use its Section 5 enforcement authority to ensure adequate protection of consumer privacy in the digital age.

Respectfully Submitted,

Marc Rotenberg,
EPIC Executive Director

Khaliah Barnes,
EPIC Associate Director and
EPIC Administrative Law Counsel

Claire Gartland,
EPIC Consumer Protection Counsel

Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)