

December 16, 2015

Office of the Secretary
Donald S. Clark
Federal Trade Commission
Room H-113
600 Pennsylvania Avenue N.W.
Washington, D.C. 20580

Submitted via <https://ftcpubcommentworks.com/ftc/crossdeviceworkshop>

Dear Mr. Clark:

The Electronic Transactions Association (“ETA”) hereby submits its comments in response to the Commission’s invitation for information on the potential benefits to consumers of cross-device tracking for advertising and marketing purposes as well as the potential privacy and security implications of such tracking. ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services, including financial institutions, transaction processors, payments networks and others. ETA has members that engage in cross-device tracking not only to better serve their customers with targeted marketing and advertisements, but also to protect their customers through the implementation of fraud prevention and authentication mechanisms.

The Chairwoman recognized in her remarks at the Commission’s November 16th Workshop that online consumer tracking is nothing new.¹ As technology has evolved and as consumers use more and different devices to access the Internet, including desktops, laptops, tablets, wearables, smartphones and smart TVs, the industry has moved beyond the use of cookies alone and now relies in addition upon deterministic and/or probabilistic methodologies to track consumer activity across devices. Both the Chairwoman and the panelists at the Workshop acknowledged the significant benefits that cross-device tracking can deliver to consumers.²

¹ Opening Remarks of FTC Chairwoman Edith Ramirez, Cross-Device Tracking: An FTC Workshop (Nov. 16, 2015).

² Transcript of the Workshop, Part 1 at 2, 8, 17-18 available at https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-1/ftc_cross-device_tracking_workshop_-_transcript_segment_1.pdf

The Benefits of Cross-Device Tracking

Cross-device tracking allows businesses to gain a more complete view of their customers or potential customers, and their likes and interests, which in turn allows the businesses to better tailor service offerings and advertisements to their customers and improve the overall consumer experience. Linking devices enables a business to recognize returning customers, no matter which device the customers use to access the business's website and enables consumers to enjoy a seamless experience across devices.

Among the most significant benefits that cross-device tracking can deliver is improved account security and fraud prevention. As consumers do more and more business online, from shopping to banking to bill paying, and use multiple devices to transact that business, the risk of identity theft, account takeover or other fraudulent activity increases. The ability to correlate transactions based on the devices used and to link the devices owned by an individual consumer provides a more comprehensive view of the consumer that can be and is used to detect fraud, authenticate transactions and alert consumers to suspicious activity.

ETA submits that while the Commission should continue to monitor the marketplace, there is no need at this point for the Commission to explore the possibility of adopting regulations to protect consumers. Industry organizations have been extremely diligent in their efforts to put into place self-regulatory principles for cross-device tracking to which their members adhere in their advertising, marketing and privacy practices. Those in the advertising and marketing industry have every incentive to ensure that consumers have positive experiences and do not lose trust in the online marketplace. And the Commission should not take any action that may hinder the ability of the electronic payments industry to take every available precaution to ensure that consumers, merchants and financial institutions are protected from fraud, including through the use of cross-device tracking. Unlike government regulation, self-regulation is nimble, adaptable, and able to protect consumers without stifling innovation and far better able to keep pace with the rapid development of the technology.

Notice, Transparency and Choice

Consumers should be notified by the companies with which they do business, the companies whose websites they visit and any other companies that track online behavior what

information the companies collect about them and how that information is used. There are several industry trade groups that have adopted and/or enforce conscientious privacy practices that their members or participants use to inform consumers of their information collection practices and to describe how such information is used and/or shared with third parties and that allow consumers to exercise control over the collection and use of information gathered about them. For example, the Digital Advertising Alliance (“DAA”) has established a very effective self-regulatory program consisting of principles and guidance that apply to data collected and used for online behavioral advertising,³ and data collected from a particular computer or device regarding Web viewing over time and across non-affiliated Web sites.⁴ The DAA has also issued guidance on how the Self-Regulatory Principles apply in the mobile environment⁵ and to data used and collected across devices.⁶ From DAA’s website, consumers can access a list of the participating companies that collect data for interest-based advertising and other purposes from the consumer’s browser and a description of what information they collect and how they use it.⁷ The DAA website also provides a means by which consumers can opt out of having their information collected and used by one or all of the participating companies.⁸ Entities participating in the self-regulatory program may also display the AdChoices icon which consumers can use to access an entity’s privacy policies and to opt out of the entity’s data

³ DAA’s Self-Regulatory Principles for Online Behavioral Advertising (July 2009).

⁴ DAA’s Multi-Site Data Principles (November 2011).

⁵ DAA’s Application of Self-Regulatory Principles to the Mobile Environment (July 2013).

⁶ DAA’s Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (November 2015).

⁷ Many ETA members participate in the DAA’s self-regulatory program and display the AdChoices icon on their websites. The list of participating companies is available at <http://www.aboutads.info/participating>.

⁸ The Consumer Choice page on DAA’s website provides a list of the participating companies that collect Web viewing data for interest-based advertising and other uses for a consumer’s computer or device, available at <http://www.aboutads.info/choices/>. Consumers are able to access those companies’ privacy policies, a description of what information they collect and a description of how they use the information from DAA’s website. Consumers also are able to opt out from the collection of Web viewing data by some or all of the participating companies. The National Advertising Initiative has a page on its website providing similar functionalities, available at <http://www.networkadvertising.org/choices/>

collection and use practices for targeted advertising. Both the Interactive Advertising Bureau (“IAB”) and the National Advertising Initiative (“NAI”) participated in the development of the DAA’s Principles.⁹ The Council of Better Business Bureaus (“CBBB”) and the Direct Marketing Association (“DMA”) monitor and enforce compliance with the Principles.¹⁰

In addition to the DAA’s Self-Regulatory Principles, the NAI has also adopted its own Code of Conduct that requires members to provide consumers notice of their information collection and use practices for interest-based advertising and the ability to opt out of having their information so collected and used.¹¹ NAI’s Code of Conduct includes sanctions for non-compliance.

The DAA’s self-regulatory principles apply to both first parties that interact with consumers and third parties that collect information through a non-affiliate’s application or from a particular device.¹² Participating companies are required to disclose on their websites that they collect multi-site data and cross-device data from a particular browser or device for use on another computer or device.¹³ NAI members are required to provide similar disclosures on their websites.¹⁴ Consumers may opt out of such data collection and use on a device by device

⁹ Also involved in the development of the principles were the American Association of Advertising Agencies, the American Advertising Federation, the Association of National Advertisers, the Council of Better Business Bureaus, and the Direct Marketing Association. See Self-Regulatory Principles for Online Behavioral Advertising; Multi-Site Data Principles; Application of Self-Regulatory Principles to the Mobile Environment; and Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices.

¹⁰ See Enforcement of the Principles, available at <http://www.aboutads.info/enforcement>

¹¹ See NAI Code of Conduct, available at <https://www.networkadvertising.org/code-enforcement/code>; NAI Mobile Application Code of Conduct, available at https://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf NAI intends to provide guidance to its members on the application of the Code of Conduct to cross-device linking practices. NAI Comments filed October 14, 2014, available at <https://www.ftc.gov/policy/public-comments/2015/10/14/comment-00051>.

¹² See DAA’s Transparency and Control for Cross-App Data. NAI’s Code of Conduct requires members to contractually require third parties that engage in interest-based advertising to comply with the notice provisions of the Code.

¹³ Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices at 3.

¹⁴ NAI Code of Conduct at 5.

basis.¹⁵ Importantly, the self-regulatory requirements of both the DAA and NAI impose the obligation on companies to seek consumers' affirmative consent to collect and use personally identifiable information, precise location information and other sensitive information for interest-based advertising.¹⁶

ETA submits that the self-regulatory principles adopted and honored by the advertising and marketing industry, including those governing cross-device tracking, have been and will continue to be effective in promoting transparency and consumer control over data collected and used for interest-based advertising. While there may always be room for improvement and enhancement, the industry has demonstrated that it is responsive. Because the technology and the means by which consumers access the Internet are constantly evolving, industry self-regulation is a far more efficient and expedient means of protecting consumer interests than government regulation which, due to the inherent delays in the legislative and rulemaking processes, may be out of date as soon as, or soon after, any legislation or rules become effective.

ETA member operating systems are designed to detect and prevent fraud in the electronic payments market. The use of cross-device tracking for user security, to identify potential fraudulent transactions or to authenticate transactions is an extremely important mechanism for addressing cybersecurity issues. To the extent that cross-device tracking is used for the authentication and verification of transactions and to prevent fraud,¹⁷ there is always the possibility that government regulation restricting the use of cross-device tracking or of data obtained through cross-device tracking may have the unintended consequence of frustrating such risk mitigation efforts. Such a result would be unfortunate and could actually be detrimental to consumers and to the economy as a whole. In the absence of solid evidence that cross-device tracking is harmful to consumers, the Commission should refrain from taking any regulatory action at this time.

¹⁵ Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices at 3-4; NAI Code of Conduct at 5-6.

¹⁶ See Application of Self-Regulatory Principles to the Mobile Environment at 21-26; Multi-Site Data Principles at 6; NAI Code at 6-7.

¹⁷ See e.g., Opening Remarks of FTC Chairwoman Edith Ramirez at 1 (“Cross-device tracking can also help companies implement fraud prevention programs, as they learn which devices typically access consumers’ accounts.”)

Mr. Donald S. Clark
December 16, 2015
Page 6

Respectfully submitted,

Scott Talbott
Senior Vice President, Government Affairs
Mary C. Albert
Director, Regulatory Affairs
Electronic Transactions Association
1101 16th Street N.W., Suite 402
Washington, D.C. 20036
(202) 677-7417