

December 16, 2015

Federal Trade Commission  
600 Pennsylvania Ave NW  
Washington, DC 20530

**RE: Follow-up Comments, Cross-Device Tracking Workshop**

The Software & Information Industry Association (SIIA) appreciates the opportunity to submit follow-up comments to the Federal Trade Commission’s (“FTC” or “Commission”) Workshop on Cross-device Tracking, on November 16, 2015. SIIA commends the Commission for examining this important issue.

SIIA is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society, including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength—software alone [contributes](#) \$425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs.

**I. Overview and benefits of cross-device linking**

Cross-device tracking, also referred to as cross-device linking or user matching, is the practice where digital content and services companies—including advertisers and platforms— can link a user to various different devices. While this can be performed in different ways, it is not an entirely new phenomenon; rather it reflects evolution from traditional cookie-based practices that originated with desktop computers and web browsers many years ago.

The impetus behind this transition is the fact that many Americans typically use multiple connected devices each day, rather than the single personal computer and browser model of several years ago when most users were relatively static in their Internet activities.<sup>1</sup> As

---

<sup>1</sup>Recent research indicates that a typical urban citizen might use up to five personal connected devices throughout the course of a day. These include a computer, smartphone, tablets, smart TVs and other connected devices and “wearables.” Pew Research Center; June 26, 2015. <http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/>

users increasingly utilize a range of devices to access many of the same online sites and services, identifying users across devices is increasingly a practice that benefits both users and online providers.

Of course, in the same way that browser cookie identification served multiple purposes, so do the modern techniques applied across devices. They range from the provision of enhanced or customized digital content services, targeted advertising, to authentication and security purposes. Similarly, in the same way that cookie usage evolved from primarily a first party mechanism to also serve third parties, cross-device linking often involves multiple sites and entities at the same time, depending on how various techniques are deployed.

As discussed thoroughly at the recent workshop, the technical aspects of cross-device linking highlighted that these technologies are not only in the early stages with limited user understanding, but also that the technologies are rapidly evolving along with technological innovations. “Deterministic” linking is performed when a publisher or platform links a consumer’s various devices to a single account through sign-in processes on each device. “Probabilistic” linking involves the collection of information such as device type, operating system, fonts, and IP address to create a “digital fingerprint” to link a user to different devices.

Also discussed somewhat at the recent Workshop, other methods of linking are being developed and deployed, such as the “co-op” model where publishers and content providers can partner to share authenticated user data—usually in a de-identified manner utilizing hashed identifiers—to help increase accuracy and fill in gaps that often exist for entities who are not obtaining sign-ins from users. The emergence of co-ops is among the more recent developments in cross-device matching, in some cases providing an alternative to sharing data with third party advertisers that might otherwise occur through probabilistic matching.

Regardless of method, providers of digital content and internet services, including many SIIA member companies, increasingly use cross-device linking for a variety of purposes. These purposes are intended to provide a better overall digital offering for consumers. Current practices reflect an effort to apply much of the same objectives achieved in a single browser setting across the evolving technology ecosystem. Cross-device linking is already an integral part of the internet ecosystem that has become more seamless for users, while operating with significant security capabilities. Following are the three key areas driving increased deployment of device-linking practices by SIIA members and other leading digital content and services companies—these practices are beneficial to users, as well as the entities providing the services:

1. **Enhanced digital services offerings and customer analytics**—The ability to match a user across their myriad connected devices is a critical function to provide users with seamless access to individually-tailored content and services, whether accessed on a computer, smartphone, tablet, smart TV, or another connected device. Whether reading the work from a digital publisher or engaging in interactive social sites or applications, the user experience is greatly enhanced by the ability to quickly obtain all of the desired information and engage in the same practices and functions quickly across devices.

Traditional customer analytics also provide an incomplete picture of the user journey and prevents proper calculation of user interactions with websites, as well as the ability to measure the effectiveness of advertising and promotions that might have originated customer interactions. For instance, without cross-device matching techniques, a user who accesses a web site from three different devices would be erroneously measured as three unique users.

Overall, without cross-device matching, the user experience of digital services offerings would be of substantially less value to consumers.

2. **Advertising revenue for digital content**—Digital advertising has long been an engine of growth for the digital economy and a crucial source of revenue for many Internet publishers and media companies who offer their information content for little or no cost to consumers. The increase in digital advertising has continued to grow strongly, with a surge in mobile advertising in 2015. According to recent research, Domestic digital advertising revenue increased by 19 percent to \$27.5 billion during the first six months of 2015. Mobile advertising has played a substantial role in this growth, growing approximately 54 percent in the first half of 2015 to \$8.2 billion—mobile advertising now represents 30 percent of all revenue generated by digital advertising.<sup>2</sup> Also, research from 2012 found that the U.S. ad-supported digital industry directly employs 2 million people.<sup>3</sup> As advertising revenue continues to shift from print and other media formats to digital media, the ability to more effectively monetize digital content is expected to further increase.
3. **Authentication and security**—It was a lot easier to protect customer transactions and enterprise data and services when employees and customers only accessed business systems and web sites through a single computer or workstation. However, the increasing number of devices and native mobile applications and mobile-Web applications often calls for strong authentication of users across devices to prevent fraud and improve compliance across each users range devices. A recent CA survey highlights multiple security concerns companies now face as a result of myriad

---

<sup>2</sup> IAB: *Digital Advertising Hits Record High of \$27.5 Billion*; Ad Age; October 21, 2015.

<sup>3</sup> *Economic Value of the Advertising-Supported Internet Ecosystem*; IAB, September 2012.

connected devices, underscoring the need for authentication that sometimes goes beyond traditional user logins with a basic username and password.<sup>4</sup> Software security applications and services are also increasingly focused on more than one user device. For instance, Internet security service providers now offer subscriptions to any of the company's security products that can be used across devices.<sup>5</sup>

## II. Policy Considerations and Recommendations

Understandably, concerns have been raised by users and privacy advocates seeking to ensure that device matching, or "tracking," does not jeopardize users' privacy. The concerns expressed thus far largely mirror those raised over cookie-based "tracking," albeit sometimes with additional complexity for providing transparency and control, depending on the method and range of entities who may partner in various device-linking or tracking methods.

In the same way that the term "tracking" did not accurately portray all practices supported by browser cookies, such is true with cross-device linking. That is, in some cases publishers and internet services may choose to deploy device-matching to simply identify users for purposes of customizing and enhancing services, or to perform analytics and authentication and security measures. As discussed above, these are among the primary benefits of cross-device linking and are likely to play an even greater role in the years ahead as adoption of internet-connected devices continues to increase towards the "Internet of Things."

While the explosion of connected devices over the last decade represents a significant leap from the single web browser interactions that defined most consumers Internet interactions decades ago, the advancement towards an even greater number of connected or "smart" devices over the next decade is inevitable. Taking this into consideration, along with dynamic and diverse characteristics of devices that are likely to be connected to internet-based content and services in the near future, it is hard for even leading technologists to predict the purposes and benefits of cross-device linking just around the corner.

As discussed at the Workshop, inadequate transparency regarding the practices of entities to match consumers with their personal devices, and to possibly collect and compile significant behavioral information from consumers, could no doubt foster substantial confusion and distrust in the connected environment. Therefore, SIIA concurs with the consensus at the Workshop that regardless of method such device-matching takes, effective transparency and control are a priority dependent on the context in which the cross-device linking or tracking occurs.

---

<sup>4</sup> *Key Authentication Considerations for Your Mobile Strategy*; CA, 2015.

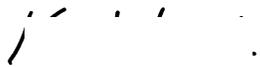
<sup>5</sup> *McAfee adds multi-factor authentication and cross-device support to all its 2016 antivirus security suites*; PC World, September 2015.

SIIA is encouraged by the recent release of guidance by the Digital Advertising Alliance (DAA) explaining how the existing Self-Regulatory Principles for Online Behavioral and Multi-Site Data, and the Application of the Self-Regulatory Principles to the Mobile Environment apply to the practice of using Multi-Site Data and Cross-App Data collected from a particular browser or device for use on a different computer or device.<sup>6</sup> This represents a timely response to demands by users and policymakers for increased transparency and control, particularly where transparency is quite limited with respect to entities working together to perform probabilistic device-matching and behavioral advertising. SIIA is committed to working with members and industry leaders across different segments of industry to encourage voluntary transparency and control regardless of the technological method used to provide cross-device linking and the gathering of associated information from consumers. For transparency and control to be effective, it must be implemented efficiently and flexibly to balance the abilities of publishers, advertisers and other entities.

Given the rapid technological evolution taking place with respect to device-matching technology, SIIA urges the FTC and policymakers to refrain from seeking new legislation or regulations to establish rigid transparency and control requirements on current or evolving device matching practices. Alternatively, policymakers should continue to encourage broad adoption of voluntary industry best-practices that provide sufficient flexibility for diverse and evolving practices. In doing so, efforts to incentive increased transparency and control should not seek to differentiate or provide a greater or lesser responsibility for transparency and control based on the type of device matching (e.g. deterministic, probabilistic, co-up or other hybrid approaches).

Again, SIIA commends the FTC for convening a discussion on this topic and for the opportunity to submit comments.

Sincerely,



Ken Wasch  
President

---

<sup>6</sup> [“Application of the Self-Regulatory Principles of Transparency and Control to Data used Across Devices,”](#) Digital Advertising Alliance, November 2015.