



October 16, 2015

Jason Kint, CEO  
Digital Content Next  
1350 Broadway, Suite 606  
New York, NY 10018

Bureau of Consumer Protection  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

**Re: FTC To Host Workshop on Cross-Device Tracking Nov. 16: Workshop Will Examine Privacy Issues That Arise As Marketers Track Consumers Across a Growing Number of Devices**

Digital Content Next (DCN) appreciates the opportunity to provide these comments in advance of the upcoming workshop regarding cross-device tracking. DCN is the only trade organization dedicated to serving the unique and diverse needs of high-quality digital content companies that manage trusted, direct relationships with consumers and marketers. DCN member companies have an audience of more than 230 million unique visitors, or 100 percent of the United States online population.<sup>1</sup> We applaud the Federal Trade Commission (FTC) for taking on the complicated issues related to cross-device tracking. We have prepared these comments to address the FTC's questions regarding the types of cross-device tracking, the risks and benefits

---

<sup>1</sup> For more information about DCN, visit <https://digitalcontentnext.org/>.

associated with it, and ways to increase transparency for consumers. Our hope is that by having a robust discussion in the early stages of this issue, we can ensure that business practices engender consumer trust.

As we have spoken and written about extensively, there is a significant lack of consumer trust across the internet ecosystem. As noted in a survey from TRUSTe earlier this year, 77% of consumers moderated their online behavior because of privacy concerns. 51% of consumers have chosen not to click on an online ad because of privacy concerns. The survey also notes that 86% of consumers took active steps to protect their privacy including deleting cookies, changing settings and turning off location tracking. Not surprisingly, more than 200 million consumers have downloaded ad blocking software.

At the same time, consumers demand and expect less friction and more convenience when they consume content or engage in an experience on platforms, websites and apps across multiple devices.

Against this backdrop, we believe it is important to focus on providing greater transparency and control for consumers with regard to cross-device tracking. Without a solid foundation built on consumer trust, the internet will never fully reach its potential.

As the FTC notes there are two kinds of cross-device tracking – deterministic and probabilistic. DCN member companies, which enjoy first-party relationships with consumers, use cross-device tracking to improve consumers' experiences and to provide seamless access to content.

Typically, publishers ask consumers to log in on a new device – thereby verifying the consumer's identity. This “deterministic” tracking allows a customer to adjust personal preferences and account settings or finish reading an article from the point at which they stopped on another device. First parties also use deterministic tracking to authenticate users more easily across devices in cases where a subscription is required or to suggest content based on customer preferences. It is important to note that deterministic tracking begins only after the consumer

logs in or proactively initiates some other form of authentication. In many cases, the consumer can choose to use the app, platform or website without logging in. In addition, responsible first parties engaged in deterministic tracking make substantial efforts to ensure their consumers understand how this tracking is conducted and for what purposes the data will be used – both in real time notices and in the privacy policy. Also, as we have noted in other FTC proceedings, consumers enjoy endless choices over where they can consume news and entertainment so they can navigate away from experiences they do not trust.

Probabilistic tracking identifies a consumer across devices based on their online behavior and common parameters like screen resolution, device type, or even battery usage.<sup>2</sup> There are many use cases for probabilistic tracking or device fingerprinting as others have termed the practice. Some third-party companies use probabilistic tracking techniques to combat online fraud and identity theft. Other companies may use probabilistic tracking techniques to gather aggregate data which is then used to understand broader consumer and industry trends. Some third parties utilize probabilistic tracking methods to serve targeted advertising. The challenge with probabilistic tracking is that consumers are often not aware their information is being collected, they don't have a relationship with the company performing the tracking and the reason for tracking may or may not fit within a reasonable consumer's expectation. Clearly, most consumers would be comfortable with data collection to combat fraud, identify theft and other crimes. Many consumers are comfortable with the collection and use of aggregate data that cannot be traced back to an individual. As the FTC has noted in other proceedings, however, many consumers are uncomfortable with non-transparent data collection that is used to build a profile about them. Even if the consumer became aware of the tracking, however, it is difficult for consumers to meaningfully exercise choice over this type of data collection. While many third party tracking services offer ways for consumers to opt out, it is challenging for consumers to understand where that choice can be exercised and often the choice is not offered within the context where the data is being collected. Indeed, even after a consumer has opted out, the consumer's choice may be lost when cookies are cleared.

---

<sup>2</sup> Natasha Lamas, [Battery Attributes Can Be Used To Track Web Users](http://techcrunch.com/2015/08/04/battery-attributes-can-be-used-to-track-web-users/), TechCrunch, August 4, 2015, <http://techcrunch.com/2015/08/04/battery-attributes-can-be-used-to-track-web-users/>

More established publishers -- those with a strong brand and online presence -- have sought to address the problem of unauthorized party data collection through the inclusion of contract terms in agreements with third parties and the other entities with whom they contract. Unfortunately, enforcement can be difficult, primarily because nearly half of all websites are not fully aware of all the tracking being conducted on their site.<sup>3</sup> New publishers, the start-up companies that are building their name for the first time through the internet, often lack bargaining power to demand contractual terms that promote stronger protection and instead have to take “off-the-rack” terms provided by intermediaries that are less restrictive in their limitations on data collection and use.

To be clear, cross-device tracking can bring substantial benefits for consumers. Deterministic tracking is typically used to enhance the consumer experience – allowing access to subscription-based content, enabling a consumer to filter or personalize their session and suggesting content are some of the use cases. Some uses of probabilistic tracking may fit within a reasonable consumer’s expectation while other uses may not and may provide zero value to the consumer.

There are also substantial risks associated with cross device tracking. Tracking across devices leads to a greater understanding of the consumer’s habits, tendencies, preferences and potentially their location and location history. This kind of data collection can be sensitive and, if it ends up in the wrong hands, could be used to harm consumers. In addition, consumers may not want to be identified on every device, platform, website or app they use. Also, many consumers choose to log in on some devices and not others – clearly demonstrating a preference not to be identified in every setting. Non-transparent cross-device tracking also presents a risk to overall consumer trust in the digital ecosystem. If consumers believe they are being ubiquitously tracked, they may curtail their online engagement in many unmeasurable ways such as by sharing less information or choosing not to buy a product. Consumers may also employ measures that hinder the functionality of the service, website or app, such as deleting all cookies or installing ad blocking software.

---

<sup>3</sup> Tony Berman, [Websites Are In The Dark About Third Party Tracking](http://www.truste.com/blog/2012/07/20/websites-are-in-the-dark-about-third-party-tracking/), TRUSTe Blog, July 20, 2012, <http://www.truste.com/blog/2012/07/20/websites-are-in-the-dark-about-third-party-tracking/>

There is likely to be significant innovation in the field of cross device tracking over the coming years, which could bring unimagined benefits to consumers and industry. However, we should be careful to safeguard the potential of cross device tracking by ensuring that all constituents provide transparency and control for consumers. DCN members go to great lengths to protect their trusted relationships with consumers and we welcome any new, innovative ways to continue educating consumers. Without consumer trust, the full benefits of the digital ecosystem cannot be realized.

DCN applauds the Commission for taking the time to study the privacy issues surrounding cross-device tracking and looks forward to collaborating with other stakeholders to ensure consumers are protected while allowing innovation to flourish.

Sincerely,

Jason Kint

CEO

Digital Content Next