Opening Remarks of FTC Chairwoman Edith Ramirez
Cross-Device Tracking: An FTC Workshop
Washington, DC
November 16, 2015

Good morning and welcome to the Federal Trade Commission's workshop on cross-device tracking.

In the early 2000s, online tracking was used primarily to determine how many individuals saw or clicked on ads. Things have changed a lot since then. Today, tracking is a much more sophisticated and complex enterprise involving a multiplicity of players as companies seek to link consumer behavior across a wide range of connected devices.

To be sure, cross-device tracking provides significant benefits to consumers. I can start reading a book on my tablet at home and then pull it up on my smartphone on the exact page I had left off if I find myself stuck in a long line somewhere. Or I can search for a pair of shoes on my home computer and then take advantage of a promotion using my smartphone when I am at the store. Cross-device tracking can also help companies implement fraud prevention programs as they learn which devices typically access consumers' accounts.

But some consumers are simply not comfortable with their browsing behavior on one device informing the ads they see on another device. And we can quickly see how our privacy might be invaded as the lines between work and home and other formerly distinct parts of our lives become increasingly blurred. Today, for example, someone who searches online about a medical condition in the privacy of her home could very well see advertisements related to that condition the next day at work or the next evening on the family's smart TV.

Many of the questions raised by cross-device tracking techniques are familiar. Are the new methods operating in a way that is transparent to consumers? Can consumers be given

effective opt-out choices? And, if not, what can be done to provide consumers with more control?

Certain attributes of cross-device tracking, however, raise additional questions and challenges. For instance, some of the techniques that companies employ to collect data passively across devices mean that online tracking is even more hidden from the typical consumer. And, as data about consumers is compiled and shared by an increasing number of companies in the tracking ecosystem – advertising firms, exchanges, and onboarding companies, just to name a few – the number of entities that have access to online information collected about consumers continues to grow.

These are some of the issues that our speakers and panelists will be addressing. Our aim is to learn more about the tracking techniques that are being used today – and those we might see tomorrow – and to discuss how we and the various players in the tracking ecosystem can address privacy risks. To set the stage for this discussion, I will begin with some background on the evolution of tracking and then highlight a few key questions about the privacy implications of cross-device tracking techniques.

I. The Evolution of Tracking

Let me start by taking you back to 2009 when the FTC issued its report on online behavioral advertising.[1] At that time, the FTC was mainly concerned with tracking across websites through cookies on a single computer. We then saw new forms of tracking emerge – first Flash cookies and then browser history "sniffing" and device "fingerprinting," among others. Last year, in our data broker report, we talked about the practice of "onboarding," where companies combine offline and online data to create even richer consumer profiles. And now,

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

we are no longer talking about tracking across a single browser on a single computer. Companies aim to follow consumers across all of their connected devices – smartphones, tablets, desktop and notebook computers, connected TVs, and even smartwatches and other wearables.

The web of linked devices, also referred to as a "device-graph," enables companies to know that multiple devices are connected to the same person. With this information, advertising can be targeted to a specific consumer across his or her devices and consumers' actions or purchases can be attributed across their interactions. As I noted earlier, I may now use my smartphone to take advantage of a shoe discount based on an ad that I saw on my home computer. Cross-device tracking and linking tells advertisers that I am likely the same person who saw the ad and made the purchase. As the number of devices we use grows, so does the degree of linking that occurs.

To do this, companies rely on what are known as "deterministic" and "probabilistic" techniques. Deterministic linking is based on information a consumer provides to a website or service, such as when they log into a social network or email account. Probabilistic models work more passively by making inferences based on information the user has no control over, such as shared IP addresses or location information when two devices are consistently used together in the same household. This approach is an example of some of the big-data techniques we highlighted last year in our big data workshop. Both methods have proven to be effective tools in tracking everything from the types of articles you read to the types of products you buy.

The experts that we have assembled today will provide additional details about the techniques companies employ to track consumers across devices.

II. Privacy-Related Challenges Raised by Cross-Device Tracking

So what privacy challenges are raised by these new and more sophisticated tracking techniques?

First and foremost, they raise important questions about transparency. While tracking itself is not new, the ways in which data is collected, compiled, stored, and analyzed certainly is. We know, for example, that behavioral techniques based on passively collected data are used to infer whether an individual might be in a particular target demographic or be interested in particular products. Now many of these same techniques are also being used to try to infer the actual identity of that individual and what devices she owns.

This more extensive tracking allows companies to connect more and more of consumers' offline activities with their online activities. This results in more detailed and more personalized consumer profiles that are assembled, traded, and shared by a growing number of entities in the data ecosystem. They do this under the veil of "anonymous identifiers" and "hashed PII," but these identifiers are still persistent and can provide a strong link to the same individual online and offline.

Not only can these profiles be used to draw sensitive inferences about consumers, there is also a risk of unexpected and unwelcome use of data generated from cross-device tracking. For example, certain data could be misused by unauthorized third parties in a way that affects consumers' access to loans, jobs, or educational opportunities. In addition, information is now often stored in large volumes for longer periods of time, thereby increasing the risk that it could be used for unexpected purposes or left vulnerable to security breaches.

Second, these concerns are exacerbated by consumers' lack of awareness of, and choices about, tracking. As it currently stands, there are almost no tools that allow individuals to know

which of their devices are linked together by tracking companies or specifically linked to them. Furthermore, while certain tools to opt out exist, most controls do not allow opting out of the underlying data collection and "linking" of identifiers; they only allow opt-outs of targeted advertising. How can companies engaged in cross-device tracking provide consumers with choices that will be honored? How will we ensure that opt-outs are effective and do not conflict with other existing controls, such as browser controls? And will industry provide an effective mechanism that allows consumers to exercise one opt-out for all devices? Understanding how different technologies work – and their limitations – is necessary to having a meaningful discussion about the notice and choice options consumers can and should have available to them in this arena.

Finally, I should note that in addition to notice and choice, we need more discussion about the role that data minimization – as well as security and accountability – play in addressing privacy concerns raised by marketing through cross-device tracking. For instance, a device-graph that probabilistically links devices as being "likely related" through tracking may quickly grow stale and may not be necessary to retain for long time periods. We should consider how these important principles can be applied in the context of cross-device tracking to mitigate privacy concerns.

III. Developing Effective Solutions

For today's workshop, we have gathered industry representatives, academics, technologists, and consumer advocates to discuss these and other implications of cross-device tracking, as well as potential solutions.

As we consider what additional steps might be necessary, the FTC will continue to monitor the marketplace and take action as needed to protect consumers. For instance, in 2011

we brought an action against online advertiser ScanScout, alleging the company had deceptively claimed consumers could opt out of tracking by changing their computer's web browser settings to block cookies.[2] We alleged that the company actually tracked consumers through Flash cookies, which consumers could not control using browser settings.

In another action in 2012, we alleged that Epic Marketplace made promises to consumers about the limited nature of its tracking when, in fact, it used "history sniffing" technology to track consumers across the Internet.[3] And, in 2013 we charged that a national company that franchised Aaron's Rent-to-Own stores engaged in an unfair practice when it did not tell consumers it could track their activities through webcams attached to their leased computers.[4] No matter what the technology, we are committed to ensuring that companies are truthful and refrain from engaging in deceptive or unfair conduct when it comes to tracking consumers.

We have also encouraged industry to adopt best practices and are pleased to see that many companies are working to differentiate themselves in the marketplace by being more privacy protective. Products touting privacy features are on the rise, and tools empowering consumers to protect their privacy, such as ad blockers, are growing in prevalence and popularity.

The Digital Advertising Alliance and the Network Advertising Initiative have also taken steps to enhance privacy protections in the online advertising space.[5] The organizations' self-regulatory principles encourage members to provide increased transparency and offer consumers

---

[2] *See ScanScout, Inc.*, No. C-4344 (F.T.C. Nov. 8, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111108scanscoutcmpt.pdf.
[3] *See Epic Marketplace, Inc.*, No. C-4389 (F.T.C. Dec. 5, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/12/121205epiccmpt.pdf.
[4] *See Aaron's, Inc.*, No. C-4442 (F.T.C. Oct. 22, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/131022aaronscmpt.pdf.
[5] *See* Digital Advertising Alliance, Digital Advertising Alliance (DAA) Self-Regulatory Program, http://www.aboutads.info; Network Advertising Initiative, Consumer Opt-Out, http://www.networkadvertising.org/choices/#completed.

control over data collection for certain practices. DAA and NAI have also developed useful opt-out tools for online data collection covered by their self-regulatory codes. NAI has also issued guidance relating to the use of non-cookie technologies, emphasizing that members should honor user opt-outs regardless of the technology used. NAI is currently developing and testing a new centralized opt-out tool that will inform consumers when NAI members use non-cookie technologies for interest-based advertising.

DAA, for its part, recently announced that it is beginning enforcement of its principles in the mobile environment.[6] It also just launched an updated version of its mobile app for Spanish speakers.[7] The app aims to provide an easy-to-use interface for consumers to set their preferences for data collection and use across apps for certain advertising and uses.

These are all steps in a positive direction. As tracking becomes more sophisticated, it is crucial that companies throughout the tracking ecosystem rise to the challenge of fostering technological solutions to inform consumers, offer choices, and honor those choices.

IV. Conclusion

We recognize that we will not be able to identify all of the potential challenges and solutions today. But this workshop is an important step forward in helping us understand how evolving tracking technologies are working so that we can move toward better safeguards and effective choices for consumers. Working through these novel and complex issues together today and in continuing conversations will help ensure that consumers' privacy interests are protected while allowing for continued innovation in the digital marketplace.

---

[6] *See* Press Release, Digital Advertising Alliance Announces Mobile Privacy Enforcement to Begin September 1 (May 7, 2015), *available* at http://www.aboutads.info/digital-advertising-alliance-announces-mobile-privacy-enforcement-begin-september-1.

[7] *See* Press Release, Digital Advertising Alliance Launches AppChoices en Español to Improve Access to DAA Mobile App for Spanish Speakers (Nov. 9, 2015), *available at* https://www.aboutads.info/digital-advertising-alliance-launches-AppChoices-en-Espanol.

Before I close, I want to acknowledge Megan Cox and the rest of the team of organizers from our Division of Privacy and Identity Protection and Office of Technology Research and Investigation for putting on today's workshop.

Thank you.