KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

October 16, 2015

Federal Trade Commission
600 Pennsylvania Avenue N.W.
Room H-113 (Annex B)
Washington, DC 20580

Re: Comments for November 2015 Workshop on Cross-Device Tracking

The Center for Democracy & Technology (CDT) is pleased to submit comments in response to the Federal Trade Commission's (FTC) call for submissions on the cross-device tracking of users by marketing firms, in anticipation of the discussion at the FTC's November 16, 2015 workshop.

Our comments focus on the following areas: the technical underpinnings of cross-device tracking; the possible benefits and drawbacks for both users and retailers; privacy and security risks that retailers should take into consideration; and possible solutions for various tracking practices.

In discussing cross-device tracking, CDT agrees that probabilistic and deterministic cross-device tracking terms are important categories for understanding the issue; however, CDT does not believe that these categories should result in different policy outcomes. In both cases users are often unaware of the wealth and detail of information that is being collected about their online and offline activities and the significant privacy invasions that result. The kind and extent of data that is recorded about users contains sensitive personally identifiable information and is often difficult or impossible for users to discover or control. For example, tracking users through the use of audio beacons allows devices in close proximity to be linked — a result completely unexpected and outside of the control of the user.

In the case of both types of tracking the best solution is increased transparency and a robust and meaningful opt-out system. If cross-device tracking companies cannot give users these types of notice and control, they should not engage in cross-device tracking. If they continue to do so then the FTC should consider whether this is an unfair practice.

TECHNICAL METHODS FOR CROSS-DEVICE TRACKING

Recently, there has been a push to track mobile devices and correlate their movements and data streams with those on the desktop. At the high level, cross-device tracking technology works by determining which user is utilizing a device, assigning that user/device pair a unique identifier, and then storing a list of these identifiers in a table.

This practice creates new privacy issues by allowing increasing aggregation of information such as an individual's location and patterns of Internet use. A typical person in an urban environment might use up to five personal connected devices throughout the course of a day: a phone, a computer, a tablet, a wearable health device, and a radio-frequency identification (RFID)-enabled access fob. Each of these devices has different purposes for the individual and each has different connectivity capabilities. As a person goes about her business, her activity on each device generates different data streams about her preferences and behavior that are siloed in these devices and services that mediate them. Cross-device tracking allows marketers to combine these streams by linking them to the same individual, enhancing the granularity of what they know about that person.

In the past there has been some geographic information leaked from a residential Internet protocol (IP) address, but it was usually limited to the city the user is in. With the advent of cell phones in the past decade, it is possible to track a user's location by examining to which cellular tower an individual's cell phone connects. Cellular phone tower tracking could generally place users in in a city. As smartphones have become popular, further granularity is available. Under ideal conditions, positioning systems utilizing Wi-Fi signal strength could provide much finer granularity location data, such as the specific address a user is located at, or even which floor or room a user is in within a building.

Similarly, marketers have previously assigned a user a unique identifier when they use the Web on a computer, and store that identifier in a browser cookie. However, due to the rise of additional devices that individuals use, the cookie model of identifying users does not work as well since cookies are specific to browsers on a given device, not to the individual using them. Because a user could search for an item using a smartphone, but later buy the item using a computer, the cookie-based model of identifying users would only capture the final stage on the computer, but not the previous session on the smartphone.

This use of multiple devices has prevented advertisers from delivering more specific and timely advertisements or tracking user behavior. Advertisers use a wide array of techniques to overcome this problem and create user/device pairings. At the most basic level, a service provider can utilize what is known as "deterministic tracking,"[1] where companies simply ask users to log into an account. Any actions performed while the user is logged into said account are then recorded. If the user is signed into the platform on different devices, the company can then track the user's activities across devices. Deterministic tracking conveys a high-degree of information to companies and it allows companies to precisely track users, but the use of this data is available

[1] Ricardo Bilton, *Cross-Device Tracking, Explained*, DIGIDAY (Aug. 21, 2015), http://digiday.com/publishers/deterministic-vs-probabilistic-cross-device-tracking-explained-normals/.

only to the company that owns the login platform (and any third parties it provides that information to).[2]

However, many websites do not provide login functionality. In these situations, advertisers use so-called "probabilistic tracking." Probabilistic cross-device tracking relies on aggregated information from multiple devices, including IP addresses, device type, Web browser, and other settings, such as a list of installed fonts, to create a "digital fingerprint" that links one individual across devices. Companies input these data points into a statistical model to infer which user is using which device. Companies use algorithms to "recognize patterns and make predictions that become stronger over time."[3] Probabilistic tracking is invisible to the user and extremely difficult for a user to control.

Signals Advertisers Use to Perform Cross-Device Tracking

While an exhaustive list of tracking technologies is beyond the scope of this comment, understanding a small subset of the techniques used to perform cross-device tracking substantially helps explain the cross-device tracking landscape.

As mentioned above, the simplest method to track users is to ask them to login when first using a new device, thus allowing the company to track the user's activity on the platform, despite the fact that an individual may utilize three different devices to interact with one platform in the course of a day. A user who has logged in on all of his or her devices can easily be tracked.

If a service does not offer user accounts, or if users do not see a reason to register, advertisers rely on probabilistic tracking. The simplest method is to assign a user a unique identification (ID), then store that ID in a cookie.

However, if the cookies are cleared, the tracking ID is lost. Locally shared objects (LSOs), also known colloquially as "flash cookies" or "supercookies,"[4] can remain on a computer even if a user tells his or her browser to delete all cookies. Additionally, websites and email marketers can use a so called "web beacon"[5] — one pixel by one pixel transparent images that are served from URLs that are unique to each user — to track who has visited a webpage or viewed an email.

While tracking technologies such as supercookies and web beacons can identify that a certain user is using a particular machine, they only provide a unique ID for a single computer. In order

[2] Laura Koulet, *Probabilistic or Deterministic*, MEDIAPOST (Aug. 4, 2015), http://www.mediapost.com/publications/article/255323/probabilistic-or-deterministic-whats-the-best-cr.html.

[3] Tyler Lochner, *'Algorithms That Learn' Catching Up to Personally Identifiable Information*, MEDIAPOST (Dec. 3, 2014), http://www.mediapost.com/publications/article/239368/algorithms-that-learn-catching-up-to-personally.html.

[4] Aleecia McDonlad & Lorrie Cranor, *A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookie*s, CARNEGIE MELLON U. (Jan. 31, 2011), www.cylab.cmu.edu/research/techreports/2011/tr_cylab11001.html.

[5] Stefanie Olsen, *Nearly Undetectable Tracking Device Raises Concern*, CNET (Jan. 2, 2002), http://www.cnet.com/news/nearly-undetectable-tracking-device-raises-concern/.

to, for example, correlate a single user's iPhone browsing and her desktop computer browsing, additional techniques must be used.

When a user has not logged into a service, and methods such as cookies, LSOs, and web bugs fail to capture a user's full online browsing activity, advertisers can use a form of probabilistic tracking called browser fingerprinting[6] to identify a user. Browser fingerprinting relies on the property of intersection[7] to infer who a user is. Modern web browsers are highly customizable. While many users may install a particular font, use a particular extension, access the web from a certain place, or visit a certain website, the chances that multiple users have the same fonts and the same extensions and visit the same site from the same connection are quite low, creating in essence a unique signal that websites can use to uniquely identify the user.

Browser fingerprinting is particularly problematic since it is effective while simultaneously being very difficult to opt out of. There are not currently any privacy enhancing technologies that fully mitigate fingerprinting. Although there are some measures that individuals can take in order to avoid deterministic tracking across devices (i.e. by signing out of programs that use the same identification for multiple applications (such as Facebook or Google), using different email addresses, or utilizing privacy enhancing technologies such as Tor[8]), it is much harder for users to avoid probabilistic tracking. The harm from the lack of an opt-out is compounded by the fact that probabilistic tracking can create a more detailed and comprehensive profile of the user.

Cross-device tracking can also be performed through the use of ultrasonic inaudible sound beacons.[9] Compared to probabilistic tracking through browser fingerprinting, the use of audio beacons is a more accurate way to track users across devices.[10] The industry leader of cross-device tracking using audio beacons is SilverPush.[11] When a user encounters a SilverPush advertiser on the web, the advertiser drops a cookie on the computer while also playing an ultrasonic audio through the use of the speakers on the computer or device.[12] The inaudible code is recognized and received on the other smart device by the software development kit installed on it.[13] SilverPush also embeds audio beacon signals into TV commercials which are "picked up silently by an app installed on a [device] (unknown to the user)."[14] The audio beacon enables

[6] Peter Eckersly, *How Unique is Your Web Browser?*, ELEC. FRONTIER FOUND. (2010), https://panopticlick.eff.org/browser-uniqueness.pdf.

[7] *Properties of Unions and Intersections of Sets*, MINN. STATE, https://www.google.com/url?q=http%3A%2F%2Fweb.mnstate.edu%2Fpeil%2FMDEV102%2FU1%2FS3%2FProperty6.htm.

[8] *What is the Tor Browser?*, TOR, https://www.torproject.org/projects/torbrowser.html.en (last visited Oct. 14, 2015).

[9] *SilverPush Launches Cross-Device Ad Targeting with Unique Audio Beacon Technology*, STEAMFEED (June 9, 2015), http://www.steamfeed.com/silverpush-launches-cross-device-ad-targeting-with-unique-audio-beacon-technology/.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] Vishal Srivastava, *Ad-Tech Startup SilverPush Grabs $1.2 Million to Develop New Television Rating Platform for Advertisers*, TECH PORTAL (Sept. 23, 2015), http://thetechportal.in/2015/09/23/silverpush-funding/.

companies like SilverPush to know which ads the user saw, how long the user watched the ad before changing the channel, which kind of smart devices the individual uses, along with other information that adds to the profile of each user that is linked across devices.[15]

The user is unaware of the audio beacon, but if a smart device has an app on it that uses the SilverPush software development kit, the software on the app will be listening for the audio beacon and once the beacon is detected, devices are immediately recognized as being used by the same individual.[16] SilverPush states that the company is not listening in the background to all of the noises occurring in proximity to the device.[17] The only factor that hinders the receipt of an audio beacon by a device is distance[18] and there is no way for the user to opt-out of this form of cross-device tracking. SilverPush's company policy is to not "divulge the names of the apps the technology is embedded,"[19] meaning that users have no knowledge of which apps are using this technology and no way to opt-out of this practice. As of April of 2015, SilverPush's software is used by 6-7 apps and the company monitors 18 million smartphones.[20]

CURRENT AND POTENTIAL USES OF CROSS-DEVICE TRACKING

Cross-device tracking has already been put into use by more than a dozen marketing firms.[21] Because "[m]any consumers search on mobile devices but buy on computers, giving advertisers the incentive to track them across multiple screens"[22], cross-device tracking serves as a powerful tool for retailers and advertisement companies. By tracking individuals across devices, marketers can create complete and detailed profiles of each individual user and recognize long-term shopping or behavioral patterns.

Although not all advertising companies are using cross-device tracking, the ability to better understand users and their buying habits is attractive because companies can demonstrate that their ad resulted in a sale instead of just a view by the user. Cross-device tracking enables companies to understand users and tailor websites and ads to fit users' needs by noting which ads lead to a sale, where ads should be placed, determine which format of a platform individuals use the most, and tailor the price of an item to suit the user.[23] Ads that are tailored and targeted for certain users generate better dividends for marketing companies because resources are not

[15] *Id.*

[16] Anthony Ha, S*ilverPush Says It's Using "Audio Beacons" for an Unusual Approach to Cross-Device Ad Targeting*, TECHCRUNCH (July 24, 2014), http://techcrunch.com/2014/07/24/silverpush-audio-beacons/.

[17] *Id.*

[18] *Id.*

[19] Shuchu Bansal, *New Ways to Count Viewers*, LIVE MINT (Apr. 15, 2015), http://www.livemint.com/Opinion/3QXskshem9l6fcbfAkqmUO/New-ways-to-count-viewers.html.

[20] *Id.*

[21] Todd Wasserman, *Why Cross-Device Tracking is the Latest Obsession for Marketers*, CAMPAIGN (Aug. 27, 2015), http://www.campaignlive.com/article/why-cross-device-tracking-latest-obsession-marketers/1361742.

[22] Adam Tanner, *How Ads Follow You from Phone to Desktop to Tablet*, MIT TECH. REV. (July 1, 2015), http://www.technologyreview.com/news/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet/.

[23] J.T. Ripton, *5 Ways Cross-Device Tracking is Already Changing Sales*, SALESFORCE (Feb. 17, 2014), https://www.salesforce.com/blog/2014/02/cross-device-tracking-changing-sales-gp.html.

wasted on ads that are uninteresting or unattractive to the user. Targeted ads are clicked on three times more often than un-targeted banner ads due to the fact that the ads are only shown to users who indicated an interest in the product by visiting a related site.[24] In addition, an advertisement campaign that uses a desktop and mobile strategy in tandem increases sales from the advertisement by 30%, as opposed to using just one or the other.[25]

In the future there is a possibility that cross-device tracking could be used to track users and build profiles for individuals using a whole range of smart devices. Cross-device tracking has primarily been used to link users across smartphones, TVs, tablets, and computers. However, the increasing use of connected wearables and other connected devices expands the reach of cross-device tracking to potentially include anything that emits a signal.[26]

The amount of data that the average American consumes across numerous devices means that many individuals in the United States will be affected by probabilistic and deterministic cross-device tracking. The average American owns four digital devices and spends sixty hours per week viewing content across devices,[27] more than half of which is viewed using smartphone applications. [28] Eighty-four percent of adults in the U.S. use the Internet (up from 52% percent in 2000).[29] According to Google, about 90% of users start an activity on one device and end on another.[30] Using probabilistic matching, one company that specializes in matching users across devices, Drawbridge, "says it has linked 1.2 billion users across 3.6 billion devices."[31] The companies that are currently linking users across devices are doing so at rates of above ninety percent accuracy.[32]

Companies are experimenting with ways to track users effectively. For instance, some companies

[24] J.J. Colao, *Ads that Follow You Home: Has Tapad Cracked the Code of Cross-Device Advertising?*, FORBES (June 10, 2013), http://www.forbes.com/sites/jjcolao/2013/05/23/ads-that-follow-you-home-has-tapad-cracked-the-code-of-cross-device-advertising/.

[25] Todd Wasserman, *supra* note 21.

[26] Allison Schiff, *A Marketer's Guide to Cross-Device Identity*, AD EXCHANGER (Apr. 9, 2015), http://adexchanger.com/data-exchanges/a-marketers-guide-to-cross-device-identity/.

[27] *The U.S. Digital Consumer Report*, NIELSEN (Feb.10, 2014), http://www.nielsen.com/us/en/insights/reports/2014/the-us-digital-consumer-report.html.

[28] Adam Leila & Andrew Lipsman, *The U.S. Mobile App Report*, COMSCORE (Aug. 21, 2014), https://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report.

[29] Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, PEW RES. CENTER (June 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/.

[30] Laurie Sullivan, *It's Not Magic, Just Cross-Device Conversion Tracking*, MEDIAPOST (July 16, 2015), http://www.mediapost.com/publications/article/254111/its-not-magic-just-cross-device-conversion-track.html.

[31] Adam Tanner, *supra* note 22.

[32] Nielson analyzed one month's worth of data from Drawbridge and found that the company's model was 97.3% accurate "in indicating a relationship between two or more devices." *Drawbridge Cross-Device Connected Consumer Graph is 97.3% Accurate*, DRAWBRIDGE (Apr. 22, 2015), http://www.drawbrid.ge/news/p/drawbridge-cross-device-connected-consumer-graph-is-973-accurate. Tapad, another cross-device tracking company, has a 91.2% accuracy in identifying related devices, according to Nielsen. *Nielson Confirms Tapad Cross-Device Accuracy at 91.2%*, TAPAD (Dec. 2, 2014), http://www.tapad.com/nielsen-study-finds-tapads-device-connections-91-2-percent-accurate/.

only track users through apps on their different devices. Tracking users only using this one method still creates detailed profiles of users, despite the fact that this method makes use of a smaller set of data. For example, one company, Flurry, embeds software in 350,000 apps on over 1.2 billion devices to track users.[33] The tracking software appears on the smartphone when the individual downloads one of the many apps Flurry uses.[34] The company recently introduced a "real-time ad marketplace to send advertisers an anonymized profile of users the moment they open an app."[35] This tool not only means that Flurry's algorithms are sophisticated enough to create profiles using instantaneous data, but also means that the profiles are generated with little human oversight. The profiles that Flurry develops by tracking users are as detailed as "wealthy bookworms who own small businesses or new mothers who travel for business and like to garden."[36] Flurry has acknowledged that the tracking software has collected more data on users than the company has utilized, but the company has elected not to use this data at this time due to privacy concerns.[37]

Another company, Adobe, is currently creating a cross-device identification system that would deterministically track users across devices in the form of a data-sharing cooperative among users. Adobe will ask partner companies for the right to use "anonymous authentication data as well as HTTP header information to build cross-device links."[38] In addition, Adobe is asking permission to use some of the user's anonymous data to deterministically track users across devices and predict connections between devices when a user has not signed into Adobe's identification system. For instance, "a participating co-op member such as Dell could opt-in to share its logged-in user data with Adobe in a hashed (i.e., anonymized form)."[39] In exchange for "exposing its proprietary linkage data to the co-op, Dell would get similar authenticated data back from all other co-op participants, helping Dell better connect the dots between its consumers/prospects and their devices."[40] Meanwhile, the other co-op members "would never have access to Dell's audience PII (personally identifiable information), targeting segments, or any other user-level data — only the linkages it has established between users and their multiple devices/browsers."[41]

PRIVACY CONCERNS

This level of detailed and pervasive surveillance creates obvious privacy issues. At a basic level it is very difficult for a user to make sensitive purchases without companies logging and tracking

[33] Claire Cain Miller & Somini Sengupta, *Selling Secrets of Phone Users to Advertisers*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html?mtrref=undefined&gwh=0B08ADE58111AF506309F12037E9A257&gwt=pay&_r=0.
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] Zach Rodgers, *Adobe Pitches Marketers on a Cross-Device Data Co-op, but Privacy is a Snag*, AD EXCHANGER (July 28, 2015), http://adexchanger.com/online-advertising/adobe-pitches-marketers-on-a-cross-device-data-coop-but-privacy-is-a-snag/.
[39] *Id.*
[40] *Id.*
[41] *Id.*

this activity. Further, when a company combines the information from the different devices, an extremely detailed picture emerges. For example, a company could see that a user searched for sexually transmitted disease (STD) symptoms on her personal computer, looked up directions to a Planned Parenthood on her phone, visits a pharmacy, then returned to her apartment. While previously the various components of this journey would be scattered among several services, cross-device tracking allows companies to infer that the user received treatment for an STD. The combination of information across devices not only creates serious privacy concerns, but also allows for companies to make incorrect and possibly harmful assumptions about individuals.

This information collection could also skew along racial lines, creating unintended racial disparities in how it is used. The number of connected devices used and content-consumption habits differ across demographic groups in the U.S.; cross-device tracking does not affect every demographic group equally. Because Asians and non-Hispanic whites are more likely to have phones and home computers that they use to connect to the Internet,[42] these populations are more likely have their data tracked across devices. However, the kinds of data individuals are providing are not identical. Although connected devices like TVs and computers provide some location data, extensive smartphone use allows for more precise location tracking throughout the day. Because the Hispanic population adopts smartphones at a higher rate than any other demographic group and watch more hours of videos on their phones and online than the average American,[43] the Hispanic population is more likely to have their location tracked throughout the day, in addition to their viewing, shopping, and app usage data. While the implication of these disparities are not yet clear, it is important to recognize that they exist and will inevitably affect how the data is used.

User understanding and transparency around cross-device tracking is also very low. In the deterministic-tracking setting, users are in a better position to control which companies track their activity since individuals can sign-out of or elect not to use platforms on their devices. By signing out of platforms like Google and Facebook, users can prevent these platforms to gather data on their online activities. However, if cross device data collectives become the norm, some of the privacy value of deterministic systems may dissipate because users will be unaware of where their data is being shared.

However, probabilistic cross-device tracking creates even greater privacy issues. It is a practice that is invisible to the user and extremely difficult for the user to control. These twin problems have led an Internet standards setting body to describe the use of this technology as "harmful to the Web."[44] It contrasts the tools for control that current cookie based tracking models allow and says:

> Unsanctioned tracking, on the other hand, has little such affordance; it is difficult (and sometimes, impossible) to detect using purely technical means in the

[42] Matt Stiles, *Census: Smartphones Bridging Digital Divide*, NAT'L PUB. RADIO (June 10, 2013), http://www.npr.org/sections/codeswitch/2013/06/10/190415432/census-smartphones-bridging-digital-divide.

[43] *Id.*

[44] *Unsanctioned Web Tracking*, W3C (July 17, 2015), http://www.w3.org/2001/tag/doc/unsanctioned-tracking/.

> browser. It stems not from a well-defined specification, but instead from exploitation of certain aspects of how the Web works.
>
> The aggregate effect of unsanctioned tracking is to undermine user trust in the Web itself. Moreover, if browsers cannot isolate activity between sites and offer users control over their data, they are unable to act as trusted agents for the user.[45]

It is clear that this type of unregulated probabilistic tracking represents a real danger not just to privacy, but the Internet itself.

Possible Solutions and Incorporating the FIPPs into Cross-Device Tracking Systems

CDT believes that the Fair Information Practice Principles (FIPPs) provide the best framework for potential solutions to the privacy issues described above. Businesses that collect data should incorporate FIPPs-based protections in order to achieve the goal of protecting user privacy and security; these protections should be incorporated at the earliest possible product development stage and not treated as an afterthought. Most importantly, cross-device tracking companies should ensure that the tracking is transparent to the user and that there is individual control. By ensuring that these two principles are employed and followed by companies, users will be provided notice that they are being tracked and given the opportunity to decide what data gets collected about them. If companies cannot provide a meaningful way to notify users of data collection and give users the opportunity to decide what, if any, data is collected about them, then the FTC should examine whether this is an unfair process under the FTC Act.

As an initial matter, CDT believes that robust transparency and opt-out consent are minimum baselines. Jonathan Mayer, a computer scientist and lawyer who studies cross-device tracking, has posed the idea that cross-device tracking should be an opt-in practice.[46] By opting in to sharing data with companies, users would be aware of how private their information is and possibly reap benefits from sharing data with marketers. Some companies are already giving users a way to monetize their data and decide whether or not to share their information. For example, Datacoup is creating a forum to allow users to aggregate their data and monetize it. Once users create a Datacoup profile and link it to their social media and financial accounts, Datacoup creates an overview of a user's data for potential data purchasers and a price is set based on how many data points a user's profile has.[47] By using Datacoup, users would be able to "understand that their digital footprint is already being tracked and sold."[48] Although no data has yet been sold in this personal data marketplace, companies like Datacoup are in discussions with data purchasers.[49] FTC should explore whether these methods are feasible.

But regardless of whether an opt-in model is possible in both the deterministic and the probabilistic settings, cross-device tracking should be regulated by the FTC to ensure that users

[45] *Id.*

[46] Allison Schiff, *supra* note 26.

[47] Aza Wee Sile, *Privacy Compromised? Might as Well Monetize*, CNBS (Jan. 30, 2015), http://www.cnbc.com/2015/01/30/privacy-compromised-might-as-well-monetize.html.

[48] *Id.*

[49] *Id.*

are informed and given a meaningful choice to protect their data. In the area of deterministic tracking, where users do have some level of control through decisions on which login platforms to use and whether to stay logged in, the FTC needs to provide guidance on the way this information is used and how the users are notified and informed of this process. Although users do have some sense that they are trading some level of privacy for a service, users are often unaware of the extent of tracking. In regard to control over tracking, the FTC should make clear that if an individual logs out of a platform on a connected device, the user should no longer be tracked by a platform while on that device. The act of logging out of a platform reflects a user's choice to no longer be tracked by the platform company, and the company should respect this decision.

Additionally, if a company plans to share the information with a third-party, either through individual sales or through a cross-device tracking data cooperative, users should be informed of this decision and given the opportunity to opt-out of the sharing of their data. As the FTC noted in a previous report, "[d]ata brokers provide data not only to end-users, but also to other data brokers…[a]ccordingly it would be virtually impossible for a user to determine how a data broker obtained his or her data."[50] Not only is it hard for users to know which data brokers have their information or how they obtained the data, but users also do not have access to the privacy policies of such third parties brokers. Lack of knowledge of third-party privacy policies impedes the individual's ability to meaningfully and knowingly opt-in to this tracking process.

As we have described above, probabilistic tracking creates even greater issues in providing meaningful transparency and control for users. CDT is unaware of the existence of any current process for users to identify when probabilistic tracking is being used or meaningfully opt out. This represents a significant infirmity for any type of privacy protection. As such, the entities engaged in probabilistic tracking merit careful scrutiny from the FTC. If transparency and control are missing, the Commission should evaluate these actors under its unfairness authority and determine if probabilistic tracking (1) "causes substantial injury to consumers", (2) the injury "is not reasonably avoidable by consumers themselves", and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition."[51]

CONCLUSION

We applaud the FTC for considering this important topic. Consideration of issues like cross-device tracking is something that a majority of Americans want.[52] In recent polls 91% of Americans feel like they have lost control over the way their personal data is collected and used.[53] As much as 86% of users have taken steps to cover their digital footprints, and most

[50] *Data Brokers: A Call for Transparency and Accountability*, FEDERAL TRADE COMM'N 12 (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[51] 15 U.S.C. § 45(n).

[52] 64% of Americans believe that the government should do more to regulate advertisers Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CENTER (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[53] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CENTER (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

individuals say they want to do more to protect their privacy, but lack the means to be anonymous online.[54] By providing meaningful industry guidance and investigating practices that are opaque to consumers, the FTC can help Americans gain further control over the privacy.

Sincerely,

/s/ Chris Calabrese
Vice President, Policy

/s/ Katherine L. McInnis
Privacy & Technology Fellow

/s/ G.S. Hans
Policy Counsel and Director, CDT-SF

/s/ Greg Norcie
Staff Technologist

[54] *Id.*