



TrackOFF

September 9, 2015

Federal Trade Commission
600 Pennsylvania Avenue N.W.
Washington, DC 20580

Re: Public Comment | FTC Workshop on Cross-Device Tracking, Nov. 16

“[U]nsanctioned tracking is actively harmful to the Web, because it is not under the control of users and not transparent.”¹

- World Wide Web Consortium (W3C), July 17, 2015

TrackOFF, LLC (“TrackOFF”)² respectfully submits these comments in response to the Federal Trade Commission’s (FTC) invitation for public comment submissions in anticipation of the agency’s November 16, 2015 Workshop on Cross-Device Tracking.

We find that cross-device tracking represents an imminent and serious threat to U.S. national security interests by unnecessarily exposing consumers’ highly sensitive behavioral data to potential compromise. This threat is highlighted by the recent cyber attacks on the Pentagon and OPM. We therefore urge the FTC to issue guidelines for the conduct of data broker and data analytics companies.

Our comments are divided into three sections: (1) the national security threat posed by cross-device tracking and its role in the mass collection of data about U.S. consumers, (2) research demonstrating that current cross-device tracking methods are not reasonably avoidable by consumers, and (3) a recommendation for the FTC use its authority to mitigate the risks discussed herein.

1. Cross-Device Tracking & U.S. National Security Interests.

The hack and exfiltration of approximately 22 million individuals’ sensitive records at the Office of Personnel Management (OPM)³ underscores that demographic and behavioral data have become high value targets for foreign intelligence organizations. Included in the records stolen from OPM are data

¹ Unsanctioned Web Tracking, <http://www.w3.org/2001/tag/doc/unsanctioned-tracking/> (last accessed July 19, 2015).

² TrackOFF develops privacy tools to protect against the latest forms of digital tracking.

³ Information about OPM Cybersecurity Incidents, <https://www.opm.gov/cybersecurity/> (last accessed July 13, 2015).



collected during background checks revealing the applicants' prior residences, contact information of friends and family, as well as mental health and criminal histories. Such data are critically important for foreign intelligence services waging Advanced Persistent Threat (APT) attacks against targets in the United States.

APT refers to a hacking technique used to compromise a network system without detection in an effort to harvest valuable data over an extended time. A report⁴ released by information security firm Mandiant in 2013 details the lifecycle of highly sophisticated APT attacks originating from China. The initial phase of the attacks rely on a method known as spear phishing, whereby the perpetrators infiltrate a company or organization by tricking a person inside the targeted network into opening a file or clicking a link in electronic correspondence (e.g., e-mail or instant message) sent from an account impersonating a real-life associate of the victim. According to Mandiant's report:

[S]pear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. [The intelligence organization] also creates webmail accounts using real peoples' names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel— and uses these accounts to send the emails.

National security experts have noted that the data stolen from OPM represent a "treasure trove" of information that can be used to gather the intelligence necessary to lodge successful spear phishing attacks. The OPM data are so sensitive, so personal, and so detailed, that they can be mined to generate highly specific, and effectively targeted, spear phishing email messages purporting to be from neighbors, workplace superiors, or old college roommates, for instance.

Yet data analytics and data broker companies maintain massive stores of sensitive, up-to-date information about U.S. citizens on a scale far larger than that of OPM.

The Commission's important investigation and May 2014 report on the practices of data brokers illustrates the sheer enormity of behavioral information held by

⁴ APT1, Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (last accessed July 13, 2015).



these companies.⁵ For example, Appendix B to the Commission’s report lists, among many other data points, that data brokers maintain the following information about U.S. consumers:

Identifying Data: Name, previously used names, address, previous addresses, e-mail address, social security number, driver’s license number, birth date, birth date of each child in a household, and birth date of family members in a house hold.

Demographic Data: Age, height, weight, gender, race & ethnicity, country of origin, religion, veteran status, and family ties.

Purchase Behavior: Types of purchases, last online order dates, guns and ammunition purchases, and types of food purchased.

Financial Data: Loans, net worth indicator, stocks and bonds owned, life insurance, and ability to afford products.

Travel Data: Date of last travel purchase, preferred airline, preferred vacation destination, and vacation property.

General Interest Data: Pets, preferred celebrities, preferred music genres, preferred movie genres, reading and listening preferences, charitable giving, and gambling behavior.

Social Media and Technology Data: Internet provider, heavy Facebook user, heavy Twitter user, uploaded pictures, and friend connections.

Health Data: Ailment and prescription online search propensity, weight loss supplements, purchase history or interest in health topics including: allergies, arthritis, medicine preferences, cholesterol, diabetes, dieting, body shaping, alternative medicine, beauty/physical enhancement, disabilities, homeopathic remedies, organic focus, orthopedics, and senior needs.

Against this backdrop it is evident that a security breach at a large data broker or data analytics company would yield an even larger “treasure trove” of information than the recent incident at OPM. In contrast to the OPM hack, however, the vast

⁵ Data Brokers, A Call for Transparency and Accountability, <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> (last accessed July 13, 2015).



majority of those affected by such a breach would have absolutely no knowledge of how their information came into the possession of these companies, nor could they have reasonably avoided such data collection practices in the first place.

2. Cookie-less Tracking Methods Are Not Reasonably Avoidable.

The FTC correctly points out in its Cross-Device Tracking Workshop proposal that new stateless forms of online tracking are beginning to replace traditional cookie-based technologies.⁶ Deterministic tracking, whereby login credentials are typically used to link an individual’s hardware devices, and probabilistic tracking, whereby the user is identified by a “digital fingerprint” comprised of unique data about a device’s hardware and software configurations, each raise serious privacy concerns. When combined, these techniques form an incredibly effective form of near-unavoidable tracking.

An example is helpful to show how this works. Our consumer privacy software, TrackOFF,⁷ applies a set of heuristics to detect and protect against specific, known fingerprinting methods. Using TrackOFF, we have identified an analytics company’s script (i.e., code) operating on four separate companies’ websites. These four websites respectively offer: (1) travel and hotel booking services, (2) weather, (3) news coverage, and (4) medical advice. See Figure 1.

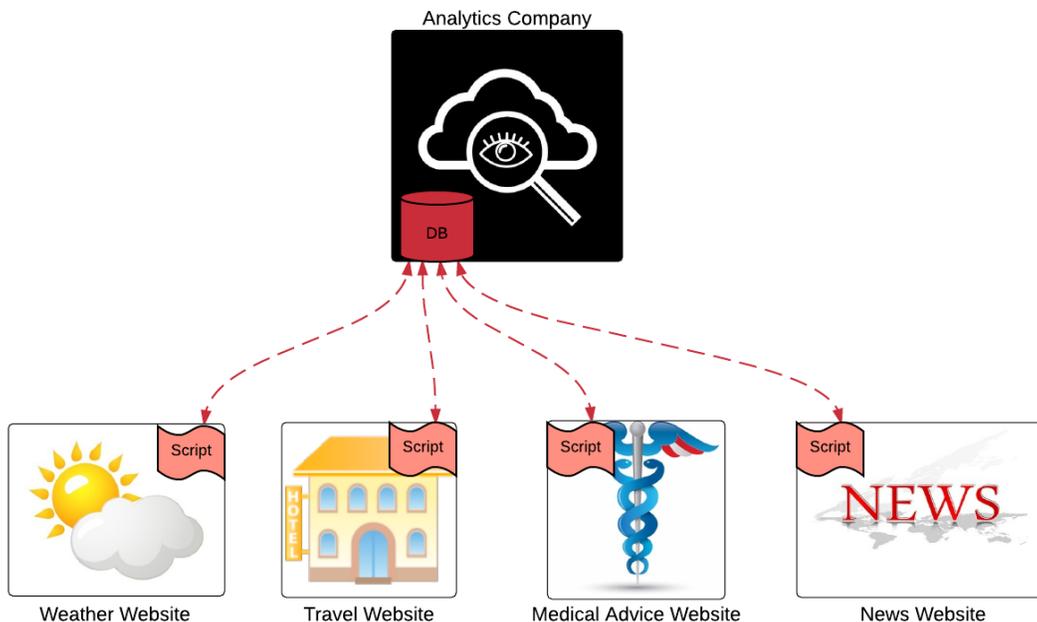


Figure 1

⁶ Cross Device Tracking, <https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking> (last accessed July 16, 2015).

⁷ TrackOFF Privacy Software, <https://www.TrackOFF.com> (last accessed July 19, 2015).



A household of four connected to a single home network is depicted in [Figure 2](#) below. The daughter, Jane Doe, uses her laptop to reserve a hotel room via the travel website. She is required to enter her e-mail address, full name, and credit card number to complete the transaction. At the same time, and without her knowledge or consent, the analytics company's script operating on the travel website captures data uniquely identifying her web browser and computer (her "digital fingerprint"). Consequently, it is now possible to link Jane's e-mail address and full name to her laptop's digital fingerprint in a custom profile stored in the analytics company's database.⁸ Her behavioral data, i.e., the city, hotel, and check-in time of her travel arrangements, may also be added to the profile.

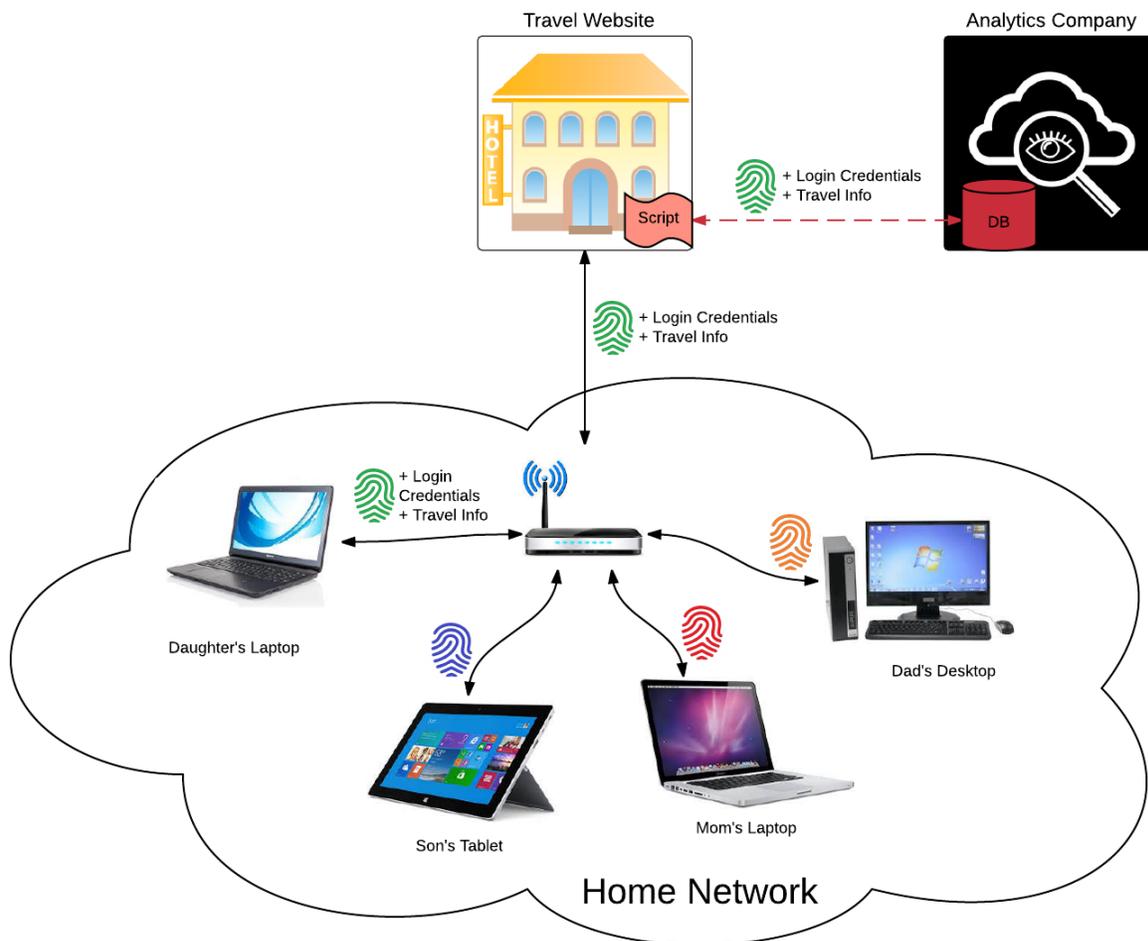


Figure 2

⁸ It is also possible that the analytics company link the daughter's digital fingerprint to her credit card number.



Figure 3 shows Jane using her laptop in a coffee shop days after booking the hotel room. She uses a search engine to research the potential causes of her persistent cough. Clicking on a link with text describing her symptoms, she is directed to the medical advice website, at which point the analytics company's script is activated and captures her digital fingerprint. The analytics company processes her digital fingerprint, and a match is returned indicating that the laptop is Jane Doe's. Thus, even without requiring Jane to log in to the medical advice website, her identity is established by the analytics company. Her profile in the analytics company's database may now be updated to include the health symptoms she searched for and viewed on the medical advice website.

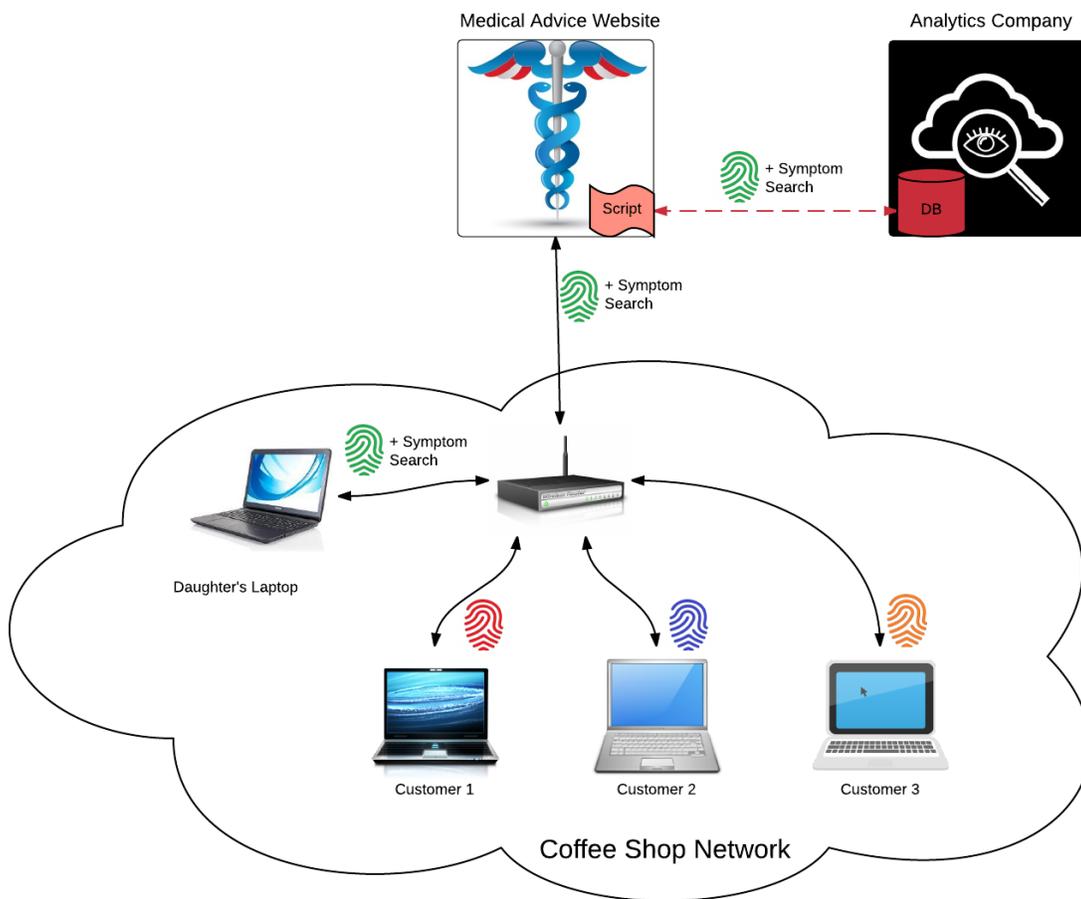


Figure 3

It follows that, even from the limited example above, the analytics company's database may now contain, among other data points associated with her laptop's IP address, the following information about Jane Doe: full name and e-mail address, upcoming travel arrangements, recently researched health symptoms, as well as a digital fingerprint uniquely identifying her laptop. In addition, if she later visits the weather or news website, her profile in the analytics company's



database may also include: the news articles she read and videos she viewed, as well as weather forecast locations she looked up. [Figure 4](#) below illustrates how these records may appear in the analytics company's database.

| Known Fingerprints | First Name | Last Name | E-mail | Device Type |
|----------------------------------|------------------|--|---|-------------|
| 3e31f4b5b0d768f8ebc528a4b61bbfa6 | Jane | Doe | jane.doe@example.com | PC |
| f45166af49d5c5bcb3de0430af7f11d3 | Jane | Doe | jane.doe@example.com | Tablet |
| Date | Website Category | Content | Activity | |
| 7/20/2015 | Travel | INFORMATION: Hotel Accommodations | ACTION TAKEN: Booked Marriott Waterfront Hotel, Baltimore, Maryland. Aug. 26-28, 2015 | |
| 7/22/2015 | Medical | RESEARCH: persistent cough, can't stop coughing | ALERT: Maladies | |
| 7/22/2015 | News | INFORMATION: Conservative news | CLICKED: Latest News from Iran US Nuclear Talks; Trump Leading in National Polls; Conservative Groups Worry About Gun Control; | |
| 7/22/2015 | Weather | INFORMATION: New York, NY | ALERT: Interest in New York City | |
| 7/23/2015 | Medical | RESEARCH: "Acetaminophen- Codeine side effects" | ALERT: Use of prescription opiates | |
| 7/25/2015 | Travel | INFORMATION: Amtrak Schedule | ACTION TAKEN: Booked Amtrak 7/30 12:00pm FROM Washington, DC to New York, NY | |

Figure 4

In practice, the steps above are repeated thousands, if not millions of time over for every person that browses the web. Furthermore, data analytics and data brokers may partner with one another to combine their profiles on individual consumers to create extremely detailed dossiers on every aspect of a person's life based on his or her web browsing behavior. Little imagination is required to understand how foreign intelligence services or other nefarious actors can use this data.

Unlike the information exposed during the OPM breach, analytics and data brokers have access to real-time data about consumers' lives—as well as their future plans. Extending the example above, assume that Jane works for manufacturer of microprocessors. It would be trivial for a malicious actor, using information misappropriated from an analytics company's database, to send Jane an e-mail from a fake but convincingly legitimate e-mail account with the subject line: "About your upcoming stay at <hotel name>!" with a malware-laden document attached showing her check-in information. If Jane opens the e-mail at work, the microprocessor manufacturer's network may be compromised.

Multiply Jane's misfortune times tens of millions of U.S. consumers, and the threat posed by cross-device tracking becomes apparent. Moreover, data analytics and data broker companies' mass data collection practices do not discriminate based on status or occupation. Any person using the web is subject to having his or her information secretly collected and stored—including legislators, teachers, engineers, nurses, judges, professors, executives, and journalists.



For illustration, consider the recent attack on the systems of the Pentagon's Joint Staff. Reports indicate that Russian hackers used a spear-phishing campaign to initially breach the Pentagon's servers before siphoning and transmitting sensitive data to thousands of accounts on the Internet.⁹ While no specifics about the victims of the spear-phishing attack have been released, it is reasonable to infer that they were targeted with e-mails containing relevant, behavioral information that induced them to open a message or attachment they otherwise would not. There is no doubt that such behavioral information about specific Pentagon employees exists within the databases of data brokers and data analytics companies.

3. Cross-Device Tracking Is Likely To Cause Substantial Injury To Consumers.

As detailed herein, because data brokers and analytics companies use highly technical and invisible measures to track user behavior across the web, the average consumer cannot reasonably avoid having his or her sensitive information collected. These actions may constitute "unfair" practices as defined by Section 5 of the FTC Act because they are likely to cause reasonably foreseeable and substantial injury to consumers, particularly in light of the recent events at OPM.

Indeed, well before the OPM incident, the Commission's report on data brokers previewed the potential injury at issue:

Although stored data may be useful for future business purposes, the risk of keeping the data may outweigh the benefits. For example, identity thieves and other unscrupulous actors may be attracted to the collection of consumer profiles that would give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, challenge questions, or other authentication credentials.¹⁰

The FTC's detailed legislative recommendations to Congress regarding the data broker industry were also commendably forward-thinking. Likely owing in part to

⁹ U.S. suspects Russia in hack of Pentagon computer network, https://www.washingtonpost.com/world/national-security/us-suspects-russia-in-hack-of-pentagon-computer-network/2015/08/06/b80e1644-3c7a-11e5-9c2d-ed991d848c48_story.html (last accessed August 7, 2015).

¹⁰ *Supra* footnote 5.



the current political climate, however, a year after the FTC's report still no reforms have materialized.

While the recently introduced Data Broker Accountability and Transparency Act (S. 668)¹¹ has the potential to effect change in the industry, the U.S. cannot afford to wait any longer to address the threat presented by mass data collection. As a result, we strongly suggest that the FTC re-issue its recommendations as guidelines for data analytics and data broker companies to begin implementing immediately. After a sufficient period of time to come into compliance, we believe that the FTC should use its authority pursuant to Section 5 of the FTC Act to prohibit data collection practices unfair to consumers.

It's important to note for completeness that data brokers and data analytics companies do provide certain valuable benefits to consumers and businesses. Examples include the facilitation of personalized offerings or helping companies understand customer preferences to better serve them. Our strong belief is that the addition of adequate transparency and consumer control mechanisms will not materially disrupt the industry's ability to continue rendering these services.

We thank the Commission for the opportunity to submit these comments, and for its continued attention and hard work on this vitally important topic.

Sincerely,

/s/

Chandler R. Givens
Co-founder & CEO
chandler@TrackOFF.com

/s/

Ryan A. Flach
Co-founder & CTO
ryan@TrackOFF.com

⦿ <https://www.TrackOFF.com> ⦿

¹¹ Data Broker Accountability and Transparency Act of 2015, <https://www.congress.gov/bill/114th-congress/senate-bill/668> (last accessed July 21, 2015).