KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

March 19, 2014

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

Re: Comments after February 2014 Workshop on Mobile 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 tracking of mobile devices by retailers, in light of the material presented and the discussion at the FTC's February 19, 2014 workshop.

Our comments focus on the following areas: the technical underpinnings of mobile device tracking; the possible benefits and drawbacks for both consumers and retailers; privacy and security risks that retailers should take into consideration; and the ideal notice and consent models for various tracking practices.

Technical Methods for Mobile Device Tracking

Retail tracking technology works by tracking individual mobile devices. Most mobile devices such as smartphones and tablets use a variety of technical means to receive and transmit data, including Bluetooth connections and WiFi access capability. Mobile devices that have WiFi or Bluetooth enabled broadcast a unique identifier (known as a MAC address) while searching for area WiFi networks or Bluetooth devices. Mobile devices also broadcast IMEI and IMSI signals in order to communicate with cellular networks, which could conceivably also be used for tracking purposes. We are not aware of any such applications at present.

Stores can monitor what MAC addresses are being broadcasted within a specific area at a particular moment, and create a profile tied to that MAC address that contains location and duration data. Using analytics software, stores can see what a particular device (and its owner) did over time within the store,[1] as well as see general customer browsing trends and traffic patterns. Because individuals tend to keep mobile devices on their person at all times, the location history of a specific device correlates with a relatively high degree of certainty to the

[1] If a business partners with another business, it may be possible to track an individual device throughout a broad range of venues. We discuss limitations on such sharing of data gathered through retail tracking with third parties below.

movement patterns of the device's owner. As a result, the location data that a business can collect from a device is often identical to the location history of its owner. This means that businesses can create a detailed profile of individual customers throughout a particular visit to a store, and potentially for *all* visits to a store – unless and until a consumer replaces her device, as MAC addresses are not easily modifiable by an individual consumer.

While most individuals will not be able to modify their MAC address on their own, there are some technical changes that could provide more effective user control. As discussed above, the design of smartphones and other mobile devices to actively search for available WiFi networks is what enables mobile device tracking by retailers. The store picks up the active search request from the phone for WiFi networks or Bluetooth devices, and collects its MAC address. But active searching for WiFi networks was never intended to be used to track an individual device over time. FTC Chief Technologist Latanya Sweeney has suggested that device manufacturers could switch to a passive probing standard,[2] which would allow devices to wait for WiFi networks to send out a beacon (rather than constantly transmit a MAC address). This would allow the device to accumulate a list of local WiFi networks, rather than give a WiFi network the ability to create a database of devices that pass through the network.

Another solution would be switching devices to *active* probing for WiFi networks in a way that would not transmit unique identifiers. As a result, consumers would have to affirmatively opt in to any tracking regimes. Devices could also be allowed to generate dynamic unique identifiers, allowing the user to change their MAC address or Bluetooth identifier and obviate persistent tracking during an extended period.

Current and Potential Uses of Mobile Tracking

At present, retail tracking technology is being developed and tested, though it has not been widely deployed.[3] According to media reports, the technology is currently being used in retail stores, stadiums, malls, airports, and other large facilities.[4] In the future, there are several ways in which businesses could create new uses for mobile device tracking. At the FTC Workshop, several panelists representing the retail sector presented possible features that could arguably provide benefits to both consumers and businesses. Retail tracking could more effectively map traffic patterns within a store, allowing managers to more efficiently schedule employees, arrange aisles and departments, and manage the flow of customers. It could also help with fraud prevention and shoplifting.

---

[2] Latanya Sweeney, *My Phone, At Your Service* (Feb. 12, 2014), http://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service.

[3] Karis Hustad, *Meet iBeacon: Location Tracking to Help You Shop*, CHRISTIAN SCIENCE MONITOR (March 16, 2014), *available at* http://www.csmonitor.com/Business/2014/0316/Meet-iBeacon-Location-tracking-to-help-you-shop.

[4] Elizabeth Dwoskin, *Site Aims to Help Users Opt Out of Smartphone Tracking*, Feb. 18, 2014 (5:34 PM), *available at* http://blogs.wsj.com/digits/2014/02/18/site-aims-to-help-users-opt-out-of-smartphone-tracking/.

Mobile tracking could also allow for targeted advertising and marketing to consumers. By observing where a specific device goes within a store, and how frequently, the retailer can target that device with coupons, advertisements, or other specials. For example, a customer who frequents the baking supply aisle in a grocery store could, over time, receive coupons for brown sugar or flour. Retailers could contend that such programs are similar to the "loyalty cards" that many stores have instituted over the last decade, in which customers scan a card upon completing a purchase. The card creates a profile of the purchases, allowing the store to track purchases over time and deliver specific coupons and other advertisements to an individual consumer. However, unlike mobile tracking, the card does not monitor where an individual consumer is in the store over time. While this practice has its proponents, several critics have observed shortcomings with loyalty programs that could easily result in the mobile tracking context. By only giving the economic benefit of coupons and reduced prices to consumers who allow their purchase history to be collected, retained, and used, retailers are effectively putting a price on their customers' privacy. This could perpetuate a social structure in which those who can afford to "pay for their privacy" receive better privacy protections over those who cannot.

Incorporating the FIPPs into Retail Tracking Systems.

As described above, because most mobile devices persistently broadcast MAC addresses in an attempt to find WiFi networks and other Bluetooth-enabled devices, retailers have access to a large amount of location data about specific devices – and by implication, their owners. The use of the FIPPs will be the most effective way to protect consumer privacy in the retail tracking context.

The policy questions raised by mobile device tracking deserve special attention by businesses as they begin to develop retail tracking systems. Businesses that collect data should incorporate FIPPs-based protections in order to achieve the goal of protecting consumer privacy and security; these protections should be incorporated at the earliest possible product development stage and not treated as an afterthought, as recent cases have shown.

At the workshop, business representatives argued for a gradual approach to instituting privacy protections (though they asserted that they take consumer privacy and security seriously). Under this approach, businesses would attempt to iterate their privacy practices over time in response the development of the technology and consumer understanding of business practices. However, we think such an approach could easily lead to the institutionalization of subpar tracking policies across the retail sector. CDT has consistently argued that new technologies do not necessarily require new solutions, and that the FIPPs are the strongest possible organizing framework for developing technologies.[5]

Recent FTC settlements indicate the need for incorporating strong standards, ideally based on the FIPPs, throughout the product development process. The FTC's settlement with Path, a mobile application development that had

[5] Comments of Center for Democracy & Technology on FTC Internet of Things Workshop (Jan. 10, 2014), *available at* https://cdt.org/files/pdfs/iot-comments-cdt-2014.pdf.

inadvertently collected address book data from users without notice and consent, highlights this need.[6] Had Path followed by privacy by design principles and carefully looked at its collection practices before releasing the app, they likely would have avoided the problem – and a hefty $900,000 fine from the FTC for violations of the FTC Act and the Children's Online Privacy Protection Act. Retail tracking companies would do well to learn from the lessons of other companies that have failed to incorporate the FIPPs into their design processes and violated long-established privacy norms when rolling out new technologies.

As with the Path settlement, other high-profile privacy and security crises that companies selling new technologies have faced in recent years could have been prevented by using the FIPPs as a privacy-protective framework. For example, the DesignerWare case, which involved laptops that inadvertently monitored consumers through the camera, could have been avoided had the retailer not supplied technology that collected private data without notice and consent to the consumer. The egregiousness of the privacy violation in that case – which in some instances captured consumers in their bedrooms engaging in intimate activities – only emphasizes the need for companies to consider limits on data collection and rigorous testing to ensure that consumers are aware of what practices are being conducted by the retailer.[7]

The FIPPs have been articulated in a number of versions in recent years, and CDT thinks that the following principles expressed by the Department of Homeland Security in 2008 are vital to any FIPPs-based framework:

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing[8]

We address each of these principles below.

Purpose Specification and Use Limitation

---

[6] United States v. Path, Inc., Consent Decree and Order for Civil Penalties, Case3:13-cv-00448-RS (Feb. 18, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

[7] *See* G.S. Hans, *Laptop Spying Case Indicates More Aggressive FTC Stance on Privacy* (Oct. 9, 2012), https://www.cdt.org/blogs/gs-hans/0910laptop-spying-case-indicates-more-aggressive-ftc-stance-privacy.

[8] Hugo Teufel III, Department of Homeland Security, *Privacy Policy Guidance Memorandum* (Dec. 29, 2008) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

Purpose specification and use limitations are vital to protecting individual privacy. Purpose specifications require companies to detail on what grounds they collect data and the uses that they plan for data; use limitations require companies to follow through on the delineated uses and refrain from using the collected data for undisclosed purposes.

Limitations on the collection of data are vitally important in a world in which increasing amounts of data can be collected from a variety of devices. Individual privacy interests are implicated at the point of collection, because of the variety of risks that databases are subject to. When a company collects data from consumers, that data can be subject to internal misuse, changes in company practices, or data breaches.[9] Some panelists at the workshop argued that relying on use limitations would be sufficient to protect consumers, but these types of threats arise long before a company actually uses the data for the purposes for which it was collected. Use limitations, while important, cannot protect against all possible threat models. As a result, purpose specification, which provides both a basis for and limits on the collection of information, is a vital element to protecting individual privacy interests. Companies engaged in retail tracking should be sure to detail the purposes for which they collect information in order to demonstrate their commitment to protecting consumers and their privacy interests.

Use limitations are also important. Companies that use mobile tracking must confine their uses of data to the purposes disclosed to consumers. If the company plans to share data collected through mobile tracking with a third party, that sharing should be disclosed to consumers, as should the third party's uses (e.g. analytics). In addition, if a company shares its data with a third party, it should consider anonymizing or pseudonymizing the data it provides in order to protect individual privacy. In its 2012 report on consumer privacy, the FTC set out the following standard to ensure that data is properly anonymized so that it cannot be "reasonably linked" to a particular consumer, computer, or device: "data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[10] CDT believes that this is an appropriate and viable standard for companies to implement to deidentify consumer data. By removing identifying information before sharing data, companies can take an affirmative step to protecting consumers even after the data is out of their direct control by reducing the likelihood that someone else can use the data for undisclosed purposes.

---

[9] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY F., *available at* http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[10] FEDERAL TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change* (February 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

In some instances, companies may change the uses of the data collected. This is a distinct possibility in the retail tracking space, as the practice is still in its infancy and companies could very well develop new uses of mobile device data in future years that are unrelated to the uses that the data was originally collected for. If that happens, companies should inform their customers and seek new consent for those new uses. Because mobile tracking is still a new retail practice, consumers have low awareness of the standard uses that companies may make of the data they collect – much less potential future uses. Therefore, the onus is on the *companies* to disclose what uses they plan to make, and, when they come up with new uses, to disclose those and re-request consent.

Transparency

Because consumers lack a strong awareness of mobile tracking due to the novelty of the practice, companies will have to educate the public on what mobile tracking is and why companies are employing it. To that end, transparency will have an important role to play in consumer education. By being transparent about their collection, use, and retention practices of mobile device data, companies will both create better public awareness of the practice and increase consumer trust by demonstrating in good faith what they do with customer data and why.

Companies will have to be deliberate in sending notices to consumers regarding their data collection and use practices. If a customer receives too many notices of company practices, they may suffer from "notice fatigue" and be unable to sift through them to determine which are vital or relevant to their individual needs. But at the very least, companies must make information about all their practices available to the public in some form – whether in a privacy policy, terms of service, or other form of detailed disclosure. The ability for the public to access information on corporate practices is vitally important, both for educational purposes and to hold companies accountable when their public statements fail to correspond with their actual practices. The FTC has entered into consent decrees with companies that have not accurately described their data privacy practices, demonstrating the need for clear disclosures to the public.[11]

Individual Participation

Related to the transparency principle, the individual participation principle urges companies to promote user participation and empowerment. The most obvious way that companies can do this is by allowing users to make decisions regarding what data gets collected, and what uses a company can make with that data, through an opt-in consent model. Because consumers purchased their mobile devices, they should be in control over what data those devices transmit. Therefore, companies should solicit the participation of consumers when seeking to access to the data that devices can provide, and consumers shouldn't have to

[11] G.S. Hans, *Goldenshores Case Demonstrates Flaws in Current Mobile Privacy Practices* (Dec. 23, 2013), *available at* https://www.cdt.org/blogs/gs-hans/2312goldenshores-case-demonstrates-flaws-current-mobile-privacy-practices.

hack their devices in order to exercise some control.[12] Because of the current system architecture of mobile phones that persistently broadcasts a MAC address (a practice that most users will not be able to disable), it is particularly important that companies that employ retail tracking solicit consumer participation in the practice, as most people will not have the ability to take steps to opt out of retail tracking on their own.

Companies that employ retail tracking collect location data from mobile devices – an especially sensitive category of data that should only be collected with affirmative, opt-in consent.[13] Notice and consent has been a bedrock principle for ensuring individual participation in transactions involving consumer data. Therefore, the development of effective notice and consent regimes will play a vital role in mobile tracking, as such tracking allows businesses to create highly granular and comprehensive records for individual customers comprised of sensitive location data. If a consumer has activated their Bluetooth and WiFi capabilities on her device, that should *not* be considered sufficient opt-in consent for the purpose of mobile device tracking.

Effective consumer notification will be necessary. Customers may not even be aware what a store collects from their phones, tablets, or wearable devices. Moreover, if stores actively probe for devices without notifying consumers, personally identifying information (such as a MAC address) could be collected from consumers without their knowledge or ability to avoid the practice. Without adequate notice and consent provisions, customers who don't approve of what a particular store does won't be able to "vote with their feet" and choose another business with better practices. Companies that employ retail tracking should provide conspicuous signage informing consumers if location information is being collected from their mobile devices. Because notice and consent in the retail context will be a challenge to implement, companies should begin developing models (such as signage, short form privacy policies, or iconography) now, rather than deploying them after they finalize their mobile tracking practices.

There are a few uses of location data gleaned from retail tracking that may not require affirmative opt-in consent – notably loss prevention and analytics. For loss prevention, it may be permissible for companies to identify particular MAC addresses that raise concerns and match all incoming MAC addresses against the problematic address. However, in such instances, stores should only check for a match against the problematic MAC address and then delete the collected MAC address without any further uses or retention of the data. This will strike an appropriate balance between protecting individual privacy and allowing businesses to use mobile device tracking for legitimate purposes.

---

[12] A recent case involving LG TVs that broadcast viewer usage practices to the manufacturer highlights the need for empowering users to make the final say over how their devices behave. *See* Justin Brookman, *Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency* (Dec. 3, 2013), *available at* https://www.cdt.org/commentary/eroding-trust-how-new-smart-tv-lacks-privacy-design-and-transparency.

[13] CDT has long advocated for opt-in consent for collection of location data, with a few narrow exceptions. *See, e.g.*, https://www.cdt.org/files/pdfs/CDT-MorrisLocationTestimony.pdf

Businesses may also seek to collect mobile device data through tracking for analytics purposes. As discussed above, many contemplated retail tracking uses depend on analyzing how individuals flow throughout a retail space over a period of time. For these types of short-term analytics uses, automatically enrolling customers but allowing them to opt-out could be justified (for example, if retailers de-identify data at the device level after each store visit). However, retaining data that could track users over multiple visits to a particular store – or between different stores – would surprise most consumers, and should only be done with their affirmative permission.

Security

The recent spate of high-profile data breaches emphasizes the need for strong security programs for all companies that collect consumer data.[14] Because mobile tracking collects sensitive data such as location information, companies should create strong security programs – and monitor and update those programs – in order to protect consumer data. Companies should be held accountable for failing to safeguard the data they maintain and should notify consumers of breaches as they occur in full compliance with current law. The failure to purge old data in accordance with minimization procedures should be a factor in evaluating whether a company's data security practices were reasonable. Although the FTC's ability to seek enforcement actions against companies for poor data security practices is currently being litigated, CDT thinks that the FTC currently has the appropriate authority under Section 5 of the FTC Act to regulate data security, and we encourage the FTC to continue to do so for companies that have substandard data security programs.[15]

As part of their security programs, companies should implement specific retention periods for data collected from mobile devices, rather than retaining that information indefinitely. CDT also supports strong de-personalization of MAC address data beyond hashing (a cryptographic technique that creates a shorter reference to the original address). As Ed Felten, a Princeton computer science professor who formerly served as the FTC's Chief Technologist, noted, merely hashing a unique identifier is not sufficient to make it anonymous.[16] By removing identifying information and deleting data after it is no longer needed, companies will both protect their customers' security and promote consumer trust by demonstrating that they are proactively protecting their pcustomers.

Data Quality and Integrity & Accountability and Auditing

Finally, companies should also ensure that the data they use and retain is accurate, relevant, and complete. Because of the sensitive nature of data collected through mobile device tracking, it is vitally important for companies to

[14] https://www.cdt.org/blogs/gs-hans/0702target-and-neiman-marcus-testify-data-breach-—-what-reforms-will-result

[15] https://www.cdt.org/blogs/gs-hans/2105data-security-and-your-next-hotel-stay-how-ftc-encourages-strong-security-practice

[16] http://techatftc.wordpress.com/2012/04/22/does-hashing-make-data-anonymous/

ensure that their records are accurate. If a promotional offer was delivered to the wrong consumer or if records were not kept suitably secure, customers could become disturbed, inconvenienced, or vulnerable to inappropriate uses.[17]

In order to ensure that data collection and use practices are followed and security programs are properly implemented, companies should create internal oversight mechanisms to promote accountability. This will ensure that the practices that companies describe to consumers are effectively followed, and will encourage consumer trust in mobile device tracking in general.

Conclusion

We thank the Commission for soliciting additional comments following the successful workshop on mobile device tracking. Despite the privacy and security risks inherent in device tracking, we believe FIPPs are as relevant as ever and that the Commission has an important role to play in terms of guidance and enforcement as device tracking practices evolve in the future.

Sincerely,

/s/
Justin Brookman
Director, Consumer Privacy Project; *CDT*

/s/
Joseph Lorenzo Hall
Chief Technologist; *CDT*

/s/
G.S. Hans
Ron Plesser Fellow; *CDT*

/s/
Runa A. Sandvik
Staff Technologist, *CDT*

[17] http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html