PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

S. 2171

THE LOCATION PRIVACY PROTECTION ACT OF 2014

Before the

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE FOR PRIVACY, TECHNOLOGY AND THE LAW

Washington, D.C.

June 4, 2014

I. Introduction

Chairman Franken, Ranking Member Flake, and members of the Subcommittee, my name is Jessica Rich, and I am the Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate this opportunity to appear before you today to discuss the Commission's efforts to protect the privacy of consumers' geolocation information and to offer initial views on the draft Location Privacy Protection Act of 2014 ("LPPA").

The LPPA addresses an important issue for the Commission, as reflected in its enforcement, policymaking, and consumer and business education efforts over a number of years: protecting the privacy of consumers' geolocation information.

This testimony first broadly discusses why precise location information is sensitive personal information and how geolocation data is used increasingly in products and services offered to consumers. Second, it highlights the Commission's recent law enforcement actions involving geolocation information.

efficient.[2] For example, consumers can get turn-by-turn directions to their destinations, find the closest bank when they are far from home, and host impromptu gatherings with friends who have "checked-in" at a certain restaurant or bar.[3]

At the same time, because geolocation information can reveal a consumer's movements in real time, as well as provide a detailed, comprehensive record of a consumer's movements over time, use of this sensitive information can raise privacy concerns.[4] Geolocation information can divulge intimately personal details about an individual. Did you visit an AIDS clinic last Tuesday? What place of worship do you attend? Were you at a psychiatrist's office last week? Did you meet with a prospective business customer?[5] Businesses can use consumers' geolocation information to build profiles of a customer's activities over time and may put the information to unanticipated uses.[6]

Sensitive geolocation information could end up in the wrong hands in a number of ways, including by being sold to companies who then use it to build profiles with other sensitive

---

[2] A number of the most popular mobile device applications ("apps") use geolocation for certain features, such as mapping and geotagging photos. *See* Matt Patronzio, *The 10 Most Popular Smartphone Apps in the U.S.* (April 3, 2014), available at http://mashable.com/2014/04/03/popular-apps-chart/.

[3] *See, e.g.*, Government Accountability Office, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy* ("GAO Mobile Device Location Report") (Sept. 2012), at 13, available at http://www.gao.gov/assets/650/648044.pdf (noting diverse array of services that make use of geolocation information for the

information, such as medical conditions or religious affiliation, without consumers' knowledge or consent, by being accessed by hackers, or by being collected through surreptitious means such as "stalking apps."[7] Given that geolocation information reveals personal information – such as where individuals live, work, or attend school – a cybercriminal could use geolocation information to facilitate social engineering or install malware or key loggers to steal a user's identity or mine credit card numbers or Social Security numbers.[8] Moreover, after obtaining an individual's geolocati

nearly three quarters of consumers surveyed were reluctant to enable location tracking on their phones due to privacy concerns.[11]

III. Enforcement

The FTC is first and foremost a civil law enforcement agency. Absent specific laws that protect geolocation information, the FTC has used its core consumer protection authority – Section 5 of the FTC Act – to enforce against unfair or deceptive practices.[12] A company acts deceptively if it makes materially misleading statements or omissions.[13] A company engages in unfair acts or practices if its practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[14] The Commission has used its enforcement authority under Section 5 to take action against companies engaged in unfair or deceptive practices involving geolocation information.

Last month, Snapchat, the developer of a popular mobile messaging app, entered into a settlement with the Commission.[15] According to the Commission's complaint, Snapchat made

multiple misrepresentations to consumers about

and shared the data automatically, thus rendering the option meaningless. The company and its manager agreed to an order that prohibits them from misrepresenting how consumers' information is collected and shared and how much control consumers have over the way their information is used. The respondents are also required to provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used, and shared, and the respondents must obtain consumers' affirmative express consent before doing so.

Finally, in a series of settlements with national rent-to-own retailer Aaron's, a company that leased software to Aaron's, and seven of Aaron's franchisees, the FTC alleged that the companies' installation and use of software on rental computers that secretly monitored and tracked consumers ran afoul of Section 5.[17] The software could log key strokes, capture screen shots, and take photographs using a computer's webcam, all unbeknownst to users. The FTC alleged that the information collected by the software revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to

[17] a atpr4(t)ocm1 96 -0m p)-6(r)io. Tf [(A)2(ar)--4.677.14.84 r3151/a-5(0ae9l r56(a)(l t5 o87( )Tj [(w(Tw

doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home. In its complaints against the companies, the FTC alleged that gathering and disclosing personal information about renters was unfair and violated the FTC Act. With respect to geolocation information, the FTC alleged that installing location tracking software on rented computers without consent from the computers' renters, tracking the geolocation of computers without notice to the computer users, and disclosing that location information to rent-to-own store licensees, caused or was likely to cause substantial injury to consumers that could not be reasonably avoided and was not outweighed by countervailing benefits to consumers or competition. Among other things, the settlement orders prohibit the companies from using monitoring software and prohibit the use of geolocation tracking without consumer consent and notice, except in cases where the device has been stolen.

IV. Policy Initiatives

In addition to the Commission's enforcement activities involving geolocation information, the Commission has conducted studies, held workshops, and issued reports on mobile privacy disclosures, mobile apps directed to kids, and other topics that elucidate best practices for companies collecting, using, and sharing information such as geolocation information.

FTC staff issued two reports about the disclosures provided in mobile apps for children: Mobile Apps for Kids: Current Privacy Disclosures are Disappointing, published in February 2012,[18] and Mobile Apps for Kids: Disclosures Still Not Making the Grade, published in

[18] FTC Staff, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (Feb. 2012), available at http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf ("First Kids' App Report").

December 2012.[19] The reports discussed what data is collected by children's apps and how it is shared, and urged industry to take steps to provide parents easier access to information about the data apps are collecting and sharing. In the February 2012 report, FTC staff surveyed the types of apps offered to children in the Apple App Store and the Android Market, and evaluated the disclosures provided to users, interactive features such as connectivity with social media, and the ratings and parental controls offered for such apps. The report noted that mobile apps can capture a broad range of user information from a mobile device automatically, including the user's precise geolocation, phone number, list of contacts, call logs, unique identifiers, and other information stored on the device. After examining the disclosures of 400 apps, FTC staff concluded that there was a lack of information available to parents prior to downloading mobile apps for their children. This was particularly problematic given the breadth of and sensitivity of the personal information apps can capture. The report called on industry to provide greater transparency about their data practices.

In December 2012, FTC staff released the results of a follow-up survey that examined whether app disclosures had improved, and whether and how apps were sharing certain types of data with third parties.[20] The survey results showed, in many instances, that apps still failed to give parents basic information about the privacy practices and interactive features of mobile apps aimed at kids. The staff found that many apps failed to provide any information about the data collected through the app, let alone the types of data collected, the purpose of the collection, and who could access to the data. Even more troubling, the results showed that many of the apps

[19] FTC Staff, Mobile Apps for Kids: Disclosures Still Not Making the Grade (Dec. 2012),

shared certain information – such as device ID, geolocation, or phone number – with third parties without disclosing that fact to parents.[21] The report urged all entities in the mobile app industry to accelerate efforts to ensure that parents have the key information they need to make decisions about the apps they download for their children.

Expanding on prior work regarding mobile disclosures, in February 2013, FTC staff issued Mobile Privacy Disclosures: Building Trust Through Transparency.[22] This staff report made recommendations for all players in the mobile marketplace – platforms, app developers, ad networks and analytics companies, and trade associations – to ensure that consumers get timely, easy

consumers, including a guide on understanding mobile apps and what information they collect from consumers.[26]

The Commission also has released guidance directed to businesses operating in the mobile arena to help educate them on best practices to handle sensitive information, such as geolocation information. The FTC published a guide, "Marketing Your Mobile App: Get It Right from the Start," to help mobile app developers observe truth-in-advertising and basic privacy principles when marketing new apps.[27] Likewise, because mobile apps and devices often rely on sensitive anLioemp o20(c(act)-e(e t)-6au)-4,halyirv,nd baobiim(he)-6(y)20(i0 Tc 152.3 [(Li)-3)-2(

protect other types of sensitive information, for example: the Gramm-Leach-Bliley Act[29] protects financial information; the Fair Credit Reporting Act[30] protects information used for

may knowingly collect or disclose geolocation information, and the Commission supports that approach.[34]

The LPPA gives the Department of Justice rulemaking authority, in consultation with the FTC, as well as sole enforcement authority. As the federal government's leading privacy enforcement agency, we recommend that the Commission be given rulemaking and enforcement authority with regard to the civil provisions of the LPPA, with DOJ exercising enforcement authority for the criminal provisions.

VII. Conclusion

Thank you for the opportunity to provide the Commission's views on privacy and geolocation information. The Commission is committed to protecting the privacy of consumers' geolocation information and we look forward to continuing to work with the Committee and