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. Third, it discusses the Commission's studies, workshops, and reports addressing geolocation privacy on mobile devices. Next, it describes the Commission's efforts to educate both businesses and consumers about the importance of reasonable privacy controls and protections for geolocation information. It concludes by providing some specific comments on the LPPA.

II. The Sensitivity of Geolocation Information

The mobile marketplace has experienced remarkable growth, with new products and services offered every day, many of which rely on consumers' geolocation information. Products and services that use geolocation information make consumers' lives easier and more

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any Commissioner.

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 13-15, *available at* http://www.gao.gov/assets/650/648044.pdf (noting diverse array of services that make use of geolocation information for the benefit of consumers).

[4] Federal Trade Commission, *Protecting Consumers in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Privacy Report") (Mar. 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.

[5] *See, e.g.*, Andrew J. Blumberg and Peter Eckersley, "On Locational Privacy, and How to Avoid Losing it Forever," Electronic Frontier Foundation (Aug. 3, 2009), *available at* https://www.eff.org/wp/locational-privacy.

[6] *See* Elizabeth Dwoskin, *What Secrets Your Phone Is Sharing About You; Businesses Use Sensors to Track Customers, Build Shopper Profiles*, WALL ST. J. (Jan. 13, 2014), *available at* http://online.wsj.com/news/articles/SB10001424052702303453004579290632128929194; Leslie Scism, *State Farm Is There: As You Drive. Insurers Use Big Data to Track Drivers, Offering Discounts as Lure, But Privacy Advocates See Dangers*, WALL ST. J. (Aug. 4, 2013), *available at* http://online.wsj.com/news/articles/SB10001424127887323420604578647950497541958 (reporting that some insurance companies are starting to provide voluntary services that use geolocation and other data points to offer better insurance rates based, at least in part, on good driving behavior).

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 geolocation information, criminals could use it to identify the individual's present or future location, thus enabling them to cause harm to an individual or his or her property, ranging from burglary and theft, to stalking, kidnapping, and domestic violence.[9]

In 2012, the Government Accountability Office ("GAO"), in a report on mobile location data, discussed consumer benefits that come with use of geolocation information – such as services that provide local weather forecasts, navigation, and retail locations – but also warned that allowing companies to access and use consumers' geolocation data exposes consumers to privacy risks, including disclosing data to unknown third parties for unspecified uses, consumer tracking, identity theft, threats to personal safety, and surveillance.[10] Likewise, many consumers are concerned about the privacy of their location data. For example, one recent study found that

---

[7] Stalking apps, which have been the subject of testimony before this Committee in the past, are apps installed on a mobile device that allow a person to monitor the device user's communications and location. Such apps can create serious safety risks for domestic violence victims whose call records, text messages, and geolocation information can be tracked by their abusers. In a similar context, the Commission has taken action against marketers of keylogger software that could, without the computer owner's consent or knowledge, record every keystroke typed on a computer. *See FTC v. CyberSpy*, No. 6:08-cv-1872-ORL-31GLK (M.D. Fla. 2010), *available at* http://www.ftc.gov/enforcement/cases-proceedings/082-3160/cyberspy-software-llc-trace-r-spence.

[8] *See* ISACA, Geolocation: Risk, Issues and Strategies (Sept. 2011), at 8, *available at* http://www.isaca.org/groups/professional-english/wireless/groupdocuments/geolocation_wp.pdf.

[9] *See id.*

[10] *See* GAO Mobile Device Location Report, *supra* note 3, at 9, 13-15.

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

---

[11] TRUSTe, *2014 U.S. Consumer Confidence Privacy Report* (Jan. 28, 2014), *available at* http://www.truste.com/about-TRUSTe/press-room/news_us_truste_reveals_consumers_more_concerned_about_data_collection; *see also* NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location* (Apr. 21, 2011), *available at* http://www.nielsen.com/us/en/newswire/2011/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location.html (finding a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device).

[12] 15 U.S.C. § 45(a). In addition, the Commission enforces the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501(8)(b), and its implementing rule, 16 C.F.R. Part 312, which includes "geolocation information" in the definition of "personal information" that child-directed websites and online services, as well as those with actual knowledge they are dealing with a child, may only collect with parental consent.

[13] *See* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

[14] *See* 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

[15] *Snapchat, Inc.*, No. 1323078 (F.T.C. May 8, 2014) (proposed consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.

multiple misrepresentations to consumers about the fundamental features of its app, including the privacy features for which it was known. The FTC alleged that Snapchat deceived consumers by promising that photo and video messages sent through the service would disappear, misrepresenting the amount of personal data it collected, and misrepresenting the security measures taken to protect that data from misuse and unauthorized disclosure. Among other things, the Commission's complaint alleged that Snapchat transmitted geolocation information from users of its Android app, even though its privacy policy claimed that it did not track users or access such information. The Commission's proposed consent order prohibits Snapchat from misrepresenting the extent to which it maintains the privacy, security, or confidentiality of users' information. In addition, the proposed order requires the company to implement a comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years.

In another case involving a mobile app developer, the FTC alleged that the developer of a flashlight app – one of the most popular apps for the Android platform, downloaded tens of million times – deceptively failed to disclose that the app transmitted the device's location, device ID, and other device data to third parties, including mobile advertising networks ("ad networks").[16] The company's privacy policy stated that it would collect "diagnostic, technical, and related" information about consumers' devices for such internal purposes as product support and software updates. The policy, however, failed to mention that the company would collect the devices' precise geolocation and persistent identifier and send them to third parties, such as ad networks. In addition, the complaint alleged that the company deceived consumers by presenting them with an option not to have their data collected or used, but nevertheless collected

[16] *Goldenshores Technologies, LLC*, No. C-4446 (F.T.C. Mar. 31, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter.

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] *Aaron's, Inc.*, No. C-4442 (F.T.C. Mar. 10, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter; *DesignerWare, LLC*, No. C-4390 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter; *Aspen Way Enterprises, Inc.*, No. C-4392 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/aspen-way-enterprises-inc-matter; *Watershed Development Corp.*, No. C- 4398 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/watershed-development-corp-matter; *Showplace, Inc.*, No. C- 4397 (F.T.C April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/showplace-inc-matter; *J.A.G. Rents, LLC*, No. C- 4395 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/jag-rents-llc-also-dba-colortyme-matter; *Red Zone Investment Group, Inc.*, No. C-4396 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/red-zone-investment-group-inc-matter; *B. Stamper Enterprises, Inc.*, No. C-4393 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/b-stamper-enterprises-inc-matter; *C.A.L.M. Ventures, Inc.*, No. C-4394 (F.T.C. April 11, 2013) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/calm-ventures-inc-matter.

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), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf ("Second Kids' App Report").

[20] The study was conducted in the Commission's mobile technology laboratory, which contains a variety of mobile devices utilizing different platforms and carriers, as well as software and equipment that permit FTC investigators to collect and preserve evidence and conduct research into a wide range of mobile issues, including those related to consumer privacy.

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-to-understand disclosures about what data companies collect and how that data is used. The report specifically discussed the need for just-in-time disclosures to consumers and obtaining affirmative express consent before allowing access to sensitive information like geolocation.

The FTC continually assesses new developments and emerging trends and threats in the privacy area. Earlier this year, the FTC hosted a "Spring Privacy Series" to examine the privacy implications of a number of new technologies in the marketplace.[23] The first seminar, held in February, included a panel of industry, technical experts, and privacy advocates and examined

---

[21] Although the results found that only 3% (12) of the apps in the study transmitted a user's geolocation, in every instance where an app transmitted geolocation, it also transmitted the user's device ID. The device ID is a persistent identifier associated with a particular mobile device. As a result, third parties, such as ad networks, that received this geolocation data could potentially add it to any data previously collected through other apps running on the same device. For example, FTC staff found that one ad network received information from 31 different apps. Two of these apps transmitted geolocation to the ad network along with a device identifier, and the other 29 apps transmitted other data (such as app name, device configuration details, and the time and duration of use) in conjunction with a device ID. The ad network could thus link the geolocation information obtained through the two apps to all the other data collected through the other 29 apps by matching the unique, persistent device ID. Second Kids' App Report, *supra* note 19, at 10.

[22] FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf ("Mobile Privacy Disclosures Report").

[23] Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues* (Dec. 2, 2013) *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

the privacy and security implications of mobile device tracking, where retailers and other companies use technology that can reveal information about consumers' visits to and movements within a location.[24] The seminar examined how mobile device tracking technologies work and how they are used; potential benefits to consumers, including improving customer flow through a store and efficient shopping and checkout; and privacy concerns, such as the lack of transparency of data collection, inability to opt-out, and potential profiling of customers' buying habits and geolocation information. FTC staff solicited public comments after the seminar, and a report summarizing the findings is forthcoming.

V. Consumer Education and Business Guidance

The Commission has long viewed consumer education and business guidance as an essential part of its consumer protection mission. In addition to our enforcement and policy work, the Commission educates consumers and businesses about protecting the privacy of consumers' geolocation information. The Commission has distributed millions of copies of educational materials for consumers and businesses to address ongoing threats to security and privacy and makes its guidance materials available online. The FTC recently released an updated version of "Net Cetera: Chatting with Kids About Being Online," our guide to help parents and other adults talk to kids about being safe, secure, and responsible online.[25] This new version deals with such topics as mobile apps and privacy, public Wi-Fi security, text message spam, and updated guidance on the Commission's COPPA Rule. Likewise, the FTC's Consumer Information website contains numerous guides on privacy and security topics salient to

[24] *See* Spring Privacy Series, *Mobile Device Tracking* (Feb. 19, 2014) *available at* http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.
[25] Net Cetera: Chatting with Kids About Being Online (Jan. 2014), *available at* https://www.consumer.ftc.gov/articles/pdf-0001-netcetera.pdf.

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 consumer data, the FTC has developed specific guidance for mobile app developers as they create, release, and monitor their apps.[28]

In addition to issuing written materials, FTC staff also has actively worked to educate mobile companies directly. For example, staff members have spoken at numerous meetings of mobile app developers to urge them to move forward on their efforts to improve transparency and address consumer privacy issues. The Commission's hope is that these tools provide guidance to companies, large and small, on how to prioritize the privacy and security of consumer information as they develop new products and services.

VI. The Location Privacy Protection Act of 2014

The Commission supports the goals of the LPPA, which chiefly seeks to improve the transparency of geolocation services and give consumers greater control over the collection of their geolocation information. Currently, in the commercial sphere, there are various laws that

---

[26] Understanding Mobile Apps (Sept. 2011), *available at* http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps.

[27] Marketing Your Mobile App: Get It Right from the Start (April 2013), *available at* http://www.business.ftc.gov/documents/bus81-marketing-your-mobile-app.

[28] Mobile App Developers: Start with Security (Feb. 2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

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 consumer reporting purposes; and the Health Insurance Portability and Accountability Act[31] protects personal health information. The LPPA represents an important step forward in protecting consumers' sensitive geolocation information.

In particular, this testimony highlights three important LPPA provisions that are consistent with the Commission's views. First, the bill defines "geolocation information" as information that is "sufficient to identify the street name and name of the city or town" in which a device is located. This definition is consistent in many respects with the Commission's COPPA Rule. The COPPA Rule requires parental consent for the collection of children's "geolocation information" that is "sufficient to identify street name and name of city or town."[32] The Commission supports the use of a consistent definition in the LPPA. Second, the LPPA requires that an entity collecting consumer geolocation information disclose its collection of such information. The Commission has recommended that companies make their data collection practices more transparent to consumers.[33] The disclosure mechanism outlined in the LPPA is an important step forward on transparency concerning the collection of geolocation information. Third, the LPPA requires affirmative express consent from consumers before a covered entity

[29] 15 U.S.C. §§ 6801-6827.
[30] 15 U.S.C. §§ 1681-1681x.
[31] 42 U.S.C. 1301 *et seq*.; *see also* 45 C.F.R Parts 160, 162 & 164.
[32] 16 C.F.R. Part 312.2.
[33] *See* Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; First Kids' App Report, *supra* note 18; Second Kids' App Report, *supra* note 19; Mobile Privacy Disclosures Report, *supra* note 22.

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 Congress on this critical issue.

[34] *See* Privacy Report, *supra* note 4, at 59 (stating that precise geolocation is sensitive information that requires extra protections, including giving consumers an opportunity to provide affirmative express consent before it is collected or used).; Mobile Privacy Disclosures Report, *supra* note 22, at 15-16 (same).