United States Government Accountability Office

Testimony

Before the Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, United States Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Wednesday, June 4, 2014

CONSUMERS' LOCATION DATA

Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers

Statement of Mark L. Goldstein, Director, Physical Infrastructure Issues

June 2014

CONSUMERS' LOCATION DATA

Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not Be Clear to Consumers

Highlights of GAO-14-649T, a testimony before the Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, United States Senate

Why GAO Did This Study

Smartphones and in-car navigation systems give consumers access to useful location-based services, such as mapping services. However, questions about privacy can arise if companies use or share consumers' location data without their knowledge.

Several agencies have responsibility to address consumers' privacy issues, including FTC, which has authority to take enforcement actions against unfair or deceptive acts or practices, and NTIA, which advises the President on telecommunications and information policy issues.

This testimony addresses (1) companies' use and sharing of consumers' location data, (2) consumers' location privacy risks, and (3) actions taken by selected companies and federal agencies to protect consumers' location privacy.

This testimony is based on GAO's September 2012 and December 2013 reports on mobile device location data and in-car location-based services and December 2012 and May 2013 updates from FTC and NTIA on their actions to respond to the 2012 report's recommendations.

What GAO Recommends

GAO made recommendations to enhance consumer protections in its 2012 report. GAO recommended, for example, that NTIA develop goals, milestones, and measures for its stakeholder initiative. NTIA stated that taking such actions is the role of the stakeholders and that its stakeholders had made progress in setting goals, milestones, and performance measures. GAO will continue to monitor this effort.

View GAO-14-649T. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

Fourteen mobile industry companies and 10 in-car navigation providers that GAO examined in its 2012 and 2013 reports—including mobile carriers and auto manufacturers with the largest market share and popular application developers—collect location data and use or share them to provide consumers with location-based services and improve consumer services. For example, mobile carriers and application developers use location data to provide social networking services that are linked to consumers' locations. In-car navigation services use location data to provide services such as turn-by-turn directions or roadside assistance. Location data can also be used and shared to enhance the functionality of other services, such as search engines, to make search results more relevant by, for example, returning results of nearby businesses.

While consumers can benefit from location-based services, their privacy may be at risk when companies collect and share location data. For example, in both reports, GAO found that when consumers are unaware their location data are shared and for what purpose data might be shared, they may be unable to judge whether location data are shared with trustworthy third parties. Furthermore, when location data are amassed over time, they can create a detailed profile of individual behavior, including habits, preferences, and routes traveled—private information that could be exploited. Additionally, consumers could be at higher risk of identity theft or threats to personal safety when companies retain location data for long periods or in a way that links the data to individual consumers. Companies can anonymize location data that they use or share, in part, by removing personally identifying information; however, in its 2013 report, GAO found that in-car navigation providers that GAO examined use different de-identification methods that may lead to varying levels of protection for consumers.

Companies GAO examined in both reports have not consistently implemented practices to protect consumers' location privacy. The companies have taken some steps that align with recommended practices for better protecting consumers' privacy. For example, all of the companies examined in both reports used privacy policies or other disclosures to inform consumers about the collection of location data and other information. However, companies did not consistently or clearly disclose to consumers what the companies do with these data or the third parties with which they might share the data, leaving consumers unable to effectively judge whether such uses of their location data might violate their privacy. In its 2012 report, GAO found that federal agencies have taken steps to address location data privacy through educational outreach events, reports with recommendations to protect consumer privacy, and guidance for industry. For example, the Department of Commerce's National Telecommunications and Information Administration (NTIA) brought stakeholders together to develop codes of conduct for industry, but GAO found this effort lacked specific goals, milestones, and performance measures, making it unclear whether the effort would address location privacy. Additionally, in response to a recommendation in GAO's 2012 report, the Federal Trade Commission (FTC) issued guidance in 2013 to inform companies of the Commission's views on the appropriate actions mobile industry companies should take to disclose their privacy practices and obtain consumers' consent.

Chairman Franken, Ranking Member Flake, and Members of the Subcommittee,

I am pleased to be here today to discuss our work on location privacy issues. Location-based services in smartphones and cars provide consumers with navigation tools and information relevant to their surroundings based on increasingly precise information about the consumer's location as determined by Global Positioning System (GPS) and other methods. In offering such services, companies can collect and retain precise data about consumers' locations. Privacy advocacy groups and policy makers have questioned whether location data that are collected and used by these companies pose privacy risks. Specifically, they have noted that location data can be used for purposes other than to provide services to the consumer, such as selling the data to others for marketing. They have also said that location data can be used to track consumers, which can in turn be used to steal their identity, stalk them, or monitor them without their knowledge. In addition, they have said that location data can be used to infer other sensitive information about individuals such as their religious affiliation or political activities.

My statement today highlights our work on: (1) companies' use and sharing of consumers' location data, (2) consumers' location privacy risks, and (3) actions taken by selected companies and federal agencies to protect consumers' location privacy. For this statement, we drew primarily from our reports on mobile device location data and in-car location-based services issued in September 2012 and December 2013, respectively.[1] For those reports, we examined privacy policies and other documentation and interviewed representatives of selected mobile industry companies and in-car navigation service companies.[2] We analyzed whether the

[1]GAO, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, GAO-12-903 (Washington, D.C.: Sept. 11, 2012) and *In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers*, GAO-14-81 (Washington, D.C.: Dec. 6, 2013).

[2]Specifically, for the 2012 mobile device report, we examined 14 mobile industry companies, comprising mobile carriers, operating system developers, and smartphone manufacturers that accounted for the largest market shares in the United States, and developers of applications that were the most popular at the time. For the 2013 in-car location-based services report, we examined 10 in-car navigation service companies, comprising auto manufacturers and portable navigation device companies that had the largest market share in the United States, and developers of widely used map and navigation applications.

selected companies' privacy policies and reported practices aligned with recommended privacy practices we identified based on our analysis of information from industry associations and privacy advocacy groups. We also reviewed documents and interviewed officials from federal agencies. Additionally, in December 2012 and May 2013, we followed up on agency actions to respond to recommendations we made in the 2012 report. Our September 2012 and December 2013 reports contain more detailed explanations of the methods used to conduct our work. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Consumers may access location-based services through smartphones or from in-car location-based services. Four types of companies are primarily responsible for smartphone products and services in the United States: mobile carriers, such as AT&T and Verizon; developers of operating systems, such as Apple's iPhone iOS and Google's Android; manufacturers, such as HTC and Samsung; and developers of applications such as games like Angry Birds, social networking applications like Facebook, or navigation tools like Google Maps. We refer to these companies as mobile industry companies. In-car location-based services are delivered by in-car communications systems known as "telematics" systems,[3] portable navigation devices, and map and navigation applications for mobile devices.

Companies can obtain location data in various ways. Mobile devices and in-car navigation devices determine location information through methods such as cell tower signal-based technologies, Wi-Fi Internet access point technology, crowd-sourced positioning, and GPS technology. Assisted-GPS (A-GPS), a hybrid technology that uses more than one data collection methodology, is also widely used. For example, companies such as Google and Apple use customer data to compile large databases

[3]Telematics systems use telecommunication networks and GPS signals to allow information, such as location data, to be communicated between a car and a service provider.

of cell tower and Wi-Fi access points. Non-carriers use these crowd-sourced location maps to determine location by analyzing which cell tower and Wi-Fi signals are received by a device. Consumers' location data are transmitted over the cellular network or Wi-Fi access points to companies providing the services. These location data may then be shared with third parties for various uses. For example, companies may choose to partner with third parties to provide a specific location-based service, such as real-time traffic information.

Several agencies have responsibility to address consumers' privacy and create related guidance. The Federal Trade Commission (FTC) has authority to enforce action against unfair or deceptive acts or practices of companies; the Federal Communications Commission (FCC) has regulatory and enforcement authority over mobile carriers; and the Department of Commerce's (Commerce) National Telecommunications and Information Administration (NTIA) advises the President on telecommunications and information policy issues. Additionally, the Department of Justice disseminates guidance on how law enforcement might request electronic evidence, such as a person's current or historical location data.

Companies Primarily Collect and Share Location Data to Provide and Improve Consumer Services

Representatives from mobile industry companies we spoke to for the September 2012 report and in-car navigation service companies we spoke to for the December 2013 report told us they primarily collect and share location data to provide location services and to improve those services. Mobile carriers and application developers offer a diverse array of services that use location information, such as services providing navigation and social networking services that are linked to consumers' locations. To provide these services, carriers and developers need to quickly and accurately determine location. Location data can also be used to enhance the functionality of other services that do not need to know the consumer's location to operate. Search engines, for example, can use location data as a frame of reference to return results that might be more relevant. For instance, if a consumer were to search for a pizza restaurant using a location-aware search engine, the top result may be a map of nearby pizza restaurants instead of the homepage of a national chain. In-car location services use location data to provide services such as turn-by-turn directions or roadside assistance. Representatives from both mobile industry companies and in-car navigation services companies told us they also use location data to improve the accuracy of their services. Representatives from some in-car navigation service companies said they share aggregated location data associated with traffic flows with third

parties to augment and improve the accuracy of real-time traffic services provided to consumers.

Additionally, as we reported in 2012, mobile industry companies can use and sell location data to target the advertising that consumers receive through mobile devices. Doing so may make an advertisement more relevant to a consumer than a non-targeted advertisement, boosting advertising revenue. Advertising is particularly important to application developers, as many developers give their products away and rely on advertising to consumers through free applications for revenue. Companies may also aggregate and store individual consumer data to create consumer profiles. Profiles can be used to tailor marketing or service performance to an individual's preferences.

Mobile industry companies and providers of in-car location services must also share consumer location data if a court finds that the information is warranted for law enforcement purposes. Because consumers generally carry their mobile devices with them, law enforcement can use device location data to determine the consumer's location. Because of this correlation, location data are valuable to law enforcement for tracking the movements of criminal suspects. Mobile carriers must comply with court orders directing the disclosure of historical location data (i.e., where the device was in the past) and in certain circumstances, real-time location data (i.e., where the device is now).[4]

Companies' Collection and Sharing of Location Data May Put Consumers' Privacy at Risk

Although consumers can benefit from location-based services designed to make their lives easier, consumers also expose themselves to privacy risks when they allow companies to access their location data. In some cases, consumers of location-based services may be unaware that companies share their location data for purposes other than providing those services. As we stated in our September 2012 and December 2013 reports, these privacy risks include, but are not limited to the following:

Disclosure to Unknown Third Parties for Unspecified Uses: According to privacy advocates, when a consumer agrees to use a service that accesses location data, the consumer is unlikely to know how

[4]However, for companies that do not retain personally identifiable location data, there are no data for law enforcement to use.

his or her location data may be used in ways beyond enabling the service itself. For example, location data may be shared with third parties unknown to the consumer. Because consumers do not know who these entities are or how they are using consumers' data, consumers may be unable to judge whether they are disclosing their data to trustworthy entities. Third parties that receive shared location information may vary in the levels of security protection they provide. If any of these entities has weak system protections, there is an increased likelihood that the information may be compromised.

Tracking Consumer Behavior: When location data are collected and shared, these data could be used in ways consumers did not intend, such as to track their travel patterns or to target consumers for unwanted marketing solicitations. Since consumers often carry their mobile devices with them and can use them for various purposes, location data along with data collected on the device may be used to form a comprehensive record upon which an individual's activities may be inferred. Amassing such data over time allows companies to create a richly detailed profile of individual behavior, including habits, preferences, and routines—private information that could be exploited. Consumers may believe that using these personal profiles for purposes other than providing a location-based service constitutes an invasion of privacy, particularly if the data are used contrary to consumers' expectations and results in unwanted solicitations or other nuisances.

Identity Theft: Criminals can use location data to steal identities when location data are disclosed, particularly when they are combined with other personal information. The risk of identity theft grows whenever entities begin to collect data profiles, especially if the information is not maintained securely. By illicitly gaining access to these profiles, criminals acquire information such as a consumer's name, address, interests, and friends' and co-workers' names. In addition, a combination of data elements—even elements that do not by themselves identify anyone, such as individual points of location data—could potentially be used in aggregate to identify or infer a consumer's behavior or patterns. Such information could be used to discern the identity of an individual. Furthermore, keeping data long-term, particularly if it is in an identifiable profile, increases the likelihood of identity theft.

Personal Security: Location data may be used to form a comprehensive record of an individual's movements and activities. If disclosed or posted, location data may be used by criminals to identify an individual's present or probable future location, particularly if the data also contain other

personally identifiable information. This knowledge may then be used to harm the individual or his property through, for instance, stalking or theft. Access to location information also raises child safety concerns as more children access mobile devices and location-based services. According to the American Civil Liberties Union (ACLU), location updates that consumers provide through social media have been linked to robberies, and GPS technology has been involved in stalking cases.

Surveillance: Law enforcement agencies can obtain location data through various methods, such as a court order, and such data can be used as evidence. However, according to a report by the ACLU, law enforcement agents could potentially track innocent people, such as those who happened to be in the vicinity of a crime or disturbance.[5] Consumers generally do not know when law enforcement agencies access their location data. In addition to information related to a crime, the location data collected by law enforcement may reveal potentially sensitive destinations, such as medical clinics, religious institutions, courts, political rallies, or union meetings.

Selected Companies Have Not Consistently Implemented Practices to Protect Consumers' Location Privacy; Federal Agencies Have Taken Actions but Federal Privacy Law Is Not Comprehensive

[5]American Civil Liberties Union of Northern California. *Location-Based Services: Time for a Privacy Check-in* (San Francisco, Calif.: November 2010).

Private Sector Entities Have Implemented Some Recommended Practices to Protect Consumers' Location Privacy, but Not Consistently

Industry and privacy advocacy groups have recommended practices for companies to follow in order to better protect consumers' privacy while using their personal information. These recommended practices include: (1) providing disclosures to consumers about data collection, use, and sharing; (2) obtaining consent and providing controls over location data; (3) having data retention practices and safeguards; and (4) providing accountability for protecting consumers' data. For the September 2012 report, we examined 14 mobile industry companies, and the for December 2013 report, we examined 10 in-car navigation services companies.[6] These companies have taken steps that are consistent with some, but not all, of the recommended practices:

Disclosures: All of the companies we examined for both reports have privacy policies, terms-of-service agreements, or other practices—such as on-screen notifications—to notify consumers that they collect location data and other personal information. However, some companies have not consistently or clearly disclosed to consumers what they are doing with these data or which third parties they may share them with. For example, most of the in-car navigation service companies we examined for the 2013 report provide broadly worded reasons for collecting location data that potentially allow for unlimited data collection and use. One of those company's terms of service states that the provided reasons for location data collection were not exhaustive. Furthermore, about half of the in-car navigation service companies' disclosures allow for sharing for location data when they are de-identified, but most of these companies' disclosures did not describe the purposes for sharing such data.

Consent and Controls: All of the companies we examined for both reports indicated they obtain consumer consent to collect location data and obtain this consent in various ways, some of which are more explicit than others. Companies also reported providing methods for consumers to control collection and use of location data, but the methods and amount of control varied. For example, most of the 14 mobile industry companies we examined for the 2012 report indicated that consumers could control smartphones' use of their location data from the phone; however, the ability to control this varied by operating system, with some providing more options. For example, the iPhone iOS operating system

[6]One company that is both an operating system developer and a provider of navigation services was examined for both the 2012 and 2013 reports.

displays a pop-up window the first time a consumer activates a new application that includes location-based services. The pop-up states that the application seeks to use the consumer's location and allows the consumer to accept or decline at that time. Similarly, Android smartphones notify consumers that an application will use location data at the time a consumer downloads a new application and seeks consumer consent through this process. Some in-car navigation systems we examined for the 2013 report use similar methods to notify consumers that they will collect location data to provide services. In contrast, other in-car navigation services obtain consent when a consumer purchases a vehicle. According to one privacy group we met with, if consent is obtained in this manner, consumers may not be as likely to review a company's stated privacy practices because they may be a part of a larger set of documentation about the vehicle. Additionally, none of the 10 in-car navigation service companies we examined allow consumers to delete the location data that are, or have been, collected.[7]

Retention and Safeguards: Officials from most of the companies we interviewed for the 2012 and 2013 reports said they kept location data only as long as needed for a specific purpose; however, in some cases, this could mean keeping location data indefinitely. Most of the privacy policies of the 14 mobile services companies we examined did not state how long companies keep location data, and there was wide variation in how long in-car navigation services companies retain vehicle-specific or personally identifiable location data when a customer requests services, ranging from not at all to up to 7 years. All the mobile industry companies we examined reported ways they safeguard consumers' personal information. However, in some cases, it was not clear whether these protections covered location data, since some privacy policies did not state whether location was considered a form of personal information. Thus it was unclear whether stated safeguards for personal information applied to location data.

As we reported in 2013, companies may safeguard location data that they use or share, in part, by de-identifying them, but companies we examined used different de-identification methods. De-identified data are stripped of

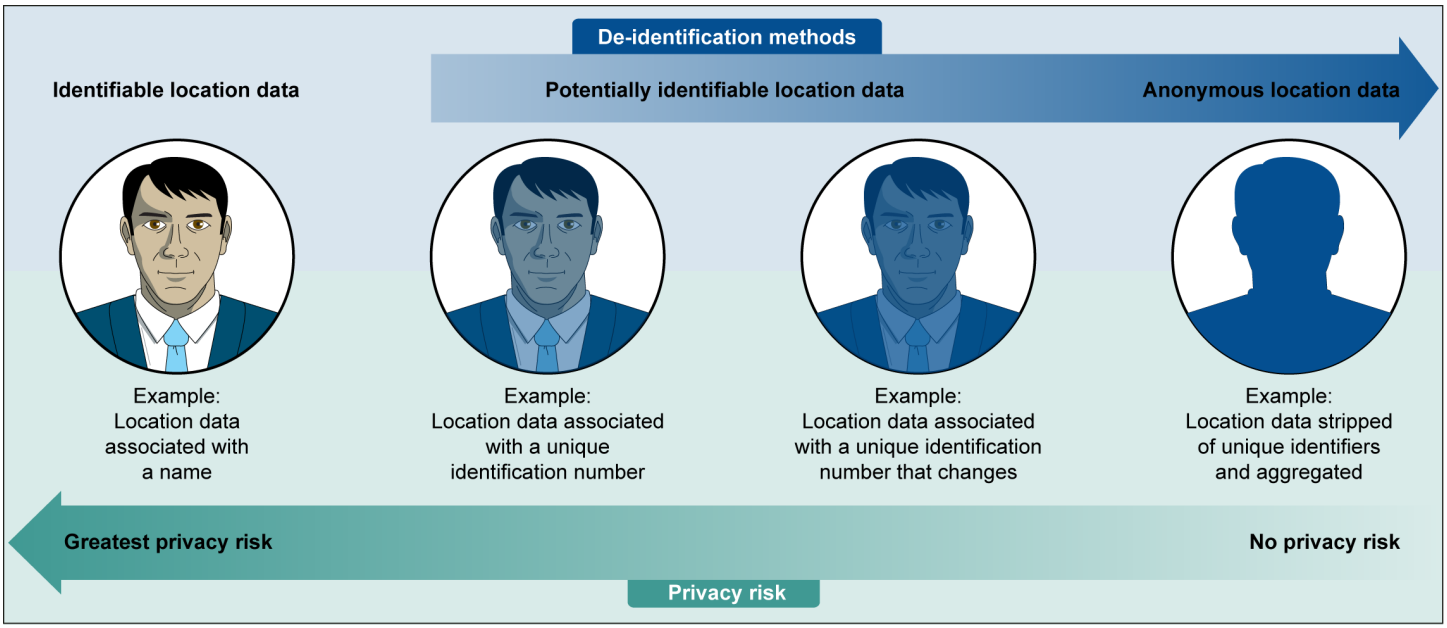
[7]We did not examine this specific issue in our 2012 report on mobile devices.

personally identifiable information.[8] The de-identification method a company uses affects the extent to which consumers may be re-identified and exposed to privacy risks. Location data that are collected along with a consumer's name or other identifying information are, by definition, personally identifiable data and present the greatest privacy risks to consumers because a consumer's identity is known. Privacy risks decrease when companies de-identify location data, but the level of risk falls on a spectrum depending on how easy it is to re-identify consumers. For example, de-identifying location data with unique identification numbers prevents the direct association of location data with a specific vehicle or individual. However, if the same identification number is re-used for the same consumer on multiple trips, then the consumer's history or patterns can potentially be discerned. Conversely, consumers face little to no privacy risks when location data are stripped of any identification numbers and aggregated with other consumers' data because the data are anonymous, meaning that the data cannot be linked to an individual at all (see fig. 1). All of the in-car navigation service companies we examined stated in their disclosures, or in interviews with us, that they use or share de-identified location data.[9]

[8]Personally identifiable information is information that is linked to a specific individual and can be used to locate or identify that person; this information includes an individual's name, aliases, Social Security number, and biometric records.

[9]We did not specifically assess the use or sharing of de-identified location data among the mobile industry companies.

Figure 1: Examples of De-Identification Methods and Privacy Risk Associated with Location-Based Data



Source: GAO.

Accountability: We reported in 2012 and 2013 that companies' accountability practices varied. For example, all 10 of the in-car navigation services companies we examined for the 2013 report stated in their disclosures or in interviews with us that they take steps to protect location data that they share with third parties. Additionally, some mobile carriers we examined for the 2012 report said they use their contracts with third parties they share consumers' personal data with to require those third parties to adhere to industry recommended practices for location data. In the 2013 report, we found that while not disclosed to consumers, representatives of in-car navigation services companies said their employees must follow the companies' internal polices to protect data, including location data, and some of the representatives further explained that employees who violate such policies are subject to disciplinary action and possibly termination. Separately, representatives from one of the in-car navigation service companies told us that it had conducted an independent audit of its practices to provide reasonable assurance that it was in line with company privacy policies. Additionally, three of the mobile industry companies we examined for the 2012 report had their privacy practices certified by TRUSTe, a company that helps companies address privacy issues by certifying businesses' privacy programs.

Lacking clear information about how companies use and share consumers' location data, consumers deciding whether to allow companies to collect, use, and share data on their location would be unable to effectively judge whether their privacy might be violated.

Federal Agencies Have Taken Actions to Protect Consumer Privacy

In our September 2012 report on mobile device location data, we reported that federal agencies that have responsibility for consumer data privacy protection have taken steps to promote awareness of privacy issues, such as providing educational outreach and recommending actions aimed at improving consumer privacy.[10] For example, in February 2012, NTIA prepared a report for the White House on protecting privacy and promoting innovation in the global digital economy.[11] The report offered a framework and expectations for companies that use personal data. The framework includes a consumer privacy bill of rights, a multistakeholder process to specify how the principles in the bill of rights apply in particular business contexts, and effective enforcement. In February 2012, FTC issued a report on privacy disclosures for mobile applications aimed at children.[12] This report highlighted the lack of information available to parents prior to downloading mobile applications for their children and called on the mobile industry to provide greater transparency about their data practices. FTC also issued a consumer privacy report in March 2012 with recommendations for companies that collect and use consumer data, including location data.[13] Finally, the Department of Justice has

[10]In the 2012 report, we also reported on three regulatory actions in the area of protecting mobile location data.

[11]The White House, *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, D.C.: Feb. 23, 2012).

[12]Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Washington, D.C.: February 2012).

[13]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C.: March 2012).

developed guidance on how law enforcement may obtain mobile location data.[14]

In our 2012 report, we concluded that NTIA and FTC could take additional actions to further protect consumers. For example, we found that NTIA had not defined specific goals, milestones, or performance measures for its proposed multistakeholder process, which consists of different groups involved with consumer privacy coming together to discuss relevant issues with the goal of developing codes of conduct for consumer privacy. Therefore, it was unclear whether the process would address location privacy. Consequently, we recommended that NTIA, in consultation with stakeholders in the multistakeholder process, develop specific goals, time frames, and performance measures for the multistakeholder process to create industry codes of conduct. In a December 2012 response to our report, the Department of Commerce (NTIA is an agency of Commerce) said it disagreed with this recommendation, stating that it is the role of the stakeholders, not the agency, to develop goals, time frames, and performance measures for the multistakeholder process. Additionally, the letter stated that stakeholders had made progress to develop their own goals, time frames, and performance measures for their efforts to create a code of conduct for mobile application transparency. We will continue to monitor NTIA's efforts in this area.

Additionally, we found that FTC had not issued comprehensive guidance to mobile industry companies with regard to actions companies should take to protect mobile location data privacy. Doing so could inform companies of FTC's views on the appropriate actions companies should take to protect consumers' mobile location privacy. We recommended that FTC consider issuing industry guidance establishing FTC's views of the appropriate actions mobile industry companies could take to protect mobile location data privacy. In February 2013, FTC issued a staff report on mobile privacy disclosures; the report provided guidance for mobile industry companies to consider when disclosing their information collection and use practices. In particular, the report suggested best practices for operating systems, application developers, advertising

[14]See, for example, Department of Justice, Executive Office for United States Attorneys. *Obtaining and Admitting Electronic Evidence* (Washington, D.C.: 2011) and Department of Justice, *Computer Crime and Intellectual Property Section Criminal Division. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Washington, D.C.: 2009).

networks and other third parties, and trade associations and other experts and researchers. For example, FTC said that operating systems should provide disclosures at the point in time when consumers access location-based services and obtain their affirmative express consent before allowing applications to access sensitive content like location data.

Federal Law Addressing Location Data Privacy Is Not Comprehensive

Currently, no comprehensive federal privacy law governs the collection, use, and sale of personal information by private-sector companies; rather, various federal laws pertain to the privacy of consumers' data:[15]

- The Federal Trade Commission Act prohibits unfair or deceptive acts or practices in or affecting commerce and authorizes FTC enforcement action.[16] This authority allows FTC to take remedial action against a company that engages in a practice that FTC has found is unfair or deceives customers. For example, FTC could take action against a company if it found the company was not adhering to the practices to protect a consumer's personal information that the company claimed to abide by in its privacy policy.
- The Electronic Communications Privacy Act of 1986 (ECPA), as amended, sets out requirements under which the government and providers of electronic communications can access and share the content of a consumer's electronic communications.[17] ECPA also prohibits providers of electronic communications from voluntarily disclosing customer records to government entities, with certain exceptions, but companies may disclose such records to a person other than government entities. The act does not specifically address whether location data are considered content or part of consumers' records. Some privacy groups have stated that ECPA should specifically address the protection of location data. The act also

[15]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[16]An act or practice is unfair if the injury it causes or is likely to cause to consumers is: (1) substantial; (2) not outweighed by countervailing benefits to consumers or to competition; and (3) not reasonably avoidable by consumers themselves. 15 U.S.C. § 45. A representation, omission, or practice is deceptive if: (1) it is likely to mislead consumers acting reasonably under the circumstances; and (2) it is material, that is, likely to affect consumers' conduct or decisions with respect to the product at issue. See e.g., Federal Trade Commission v. Patriot Alcohol Testers, Inc., 798 F. Supp. 851 (D. Mass. 1992).

[17]See, e.g., 18 U.S.C. §§ 2702, 2511.

provides legal procedures for obtaining court orders to acquire information relevant to a law enforcement inquiry.

- The Communications Act of 1934 (Communications Act), as amended, imposes a duty on telecommunications carriers to secure information and imposes particular requirements for protecting information identified as customer proprietary network information (CPNI), including the location of customers when they make calls.[18]The Communications Act requires that companies obtain express authorization from consumers before they access or disclose call location information, subject to certain exceptions.[19] Carriers must also comply with FCC rules implementing the E911 requirements of the Wireless Communications and Public Safety Act of 1999,[20] including providing location information to emergency responders when mobile phone consumers dial 911.[21]

We have previously concluded that the current privacy framework warrants reconsideration in relation to a number of issues. In our 2013 report on consumer data collected and shared by information resellers[22], we found that changes in technology and the marketplace have vastly increased the amount and nature of personal information, including location data that are collected, used, and shared. We reported that while some stakeholders' views differed, the current statutory framework does not fully address these changes. Moreover, we reported that while current laws protect privacy interests in specific sectors and for specific uses, consumers have little control over how their information is collected, used, and shared with third parties. This includes consumers' ability to access, correct, and control their personal information used for marketing, such as location data, and privacy controls related to the use of new technologies and applications, such as mobile and in-car navigation devices. In 2012,

[18]CPNI includes information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service as well as information contained in the bills pertaining to telephone service. As the Communications Act requirements for CPNI apply only to carriers, they would not apply to other types of companies that collect and use mobile phone location data, such as application developers. 47 U.S.C. § 222(f), (h).

[19]47 U.S.C. §222(f)(1).

[20]Pub. L. No. 106-81 (Oct. 26, 1999).

[21]47 C.F.R. § 20.18.

[22]GAO-13-663.

FTC and NTIA called on Congress to pass data privacy legislation that would provide a minimum level of protection for consumer data, including location data. Some Members of Congress have introduced legislative proposals that address the privacy of consumers' location data.[23]

Chairman Franken, Ranking Member Flake, and Members of the Subcommittee, this concludes my prepared remarks. I am happy to respond to any questions that you or other Members of the Subcommittee may have at this time.

GAO Contact and Staff Acknowledgement

For questions about this statement, please contact Mark L. Goldstein, Director, Physical Infrastructure Issues, at (202) 512-2834 or goldsteinm@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this statement include Andrew Von Ah (Assistant Director), Michael Clements, Roshni Davé, Colin Fallon, Andrew Huddleston, Lori Rectanus, and Crystal Wesco.

[23]See e.g., S. 2171, 113th Cong. (2014); S. 639, 113th Cong. (2013); H.R. 1312, 113th Cong. (2013).