

GAO

Report to the Chairman, Subcommittee
on Privacy, Technology and the Law,
Committee on the Judiciary, U.S.
Senate

September 2012

MOBILE DEVICE LOCATION DATA

Additional Federal Actions Could Help Protect Consumer Privacy



G A O

Accountability * Integrity * Reliability

Highlights of [GAO-12-903](#), a report to the Chairman, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

Smartphones can provide services based on consumers' location, raising potential privacy risks if companies use or share location data without consumers' knowledge. FTC enforces prohibitions against unfair and deceptive practices, and NTIA sets national telecommunications policy. GAO was asked to examine this issue. GAO reviewed (1) how mobile industry companies collect location data, why they share these data, and how this affects consumers; (2) actions private sector entities have taken to protect consumers' privacy and ensure security of location data; and (3) actions federal agencies have taken to protect consumer privacy and what additional federal efforts, if any, are needed. GAO analyzed policies and interviewed representatives of mobile industry companies, reviewed documents and interviewed officials from federal agencies, and interviewed representatives from industry associations and privacy advocates.

What GAO Recommends

GAO recommends that NTIA work with stakeholders to outline specific goals, milestones, and performance measures for its process to develop industry codes of conduct and that FTC consider issuing guidance on mobile companies' appropriate actions to protect location data privacy. Because the agencies had concerns about certain aspects of GAO's draft recommendations, GAO revised them by including that NTIA should work with stakeholders in the process to develop industry codes and removing from the draft FTC recommendation that the guidance should include how FTC will enforce the prohibition against unfair practices.

View [GAO-12-903](#). For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

MOBILE DEVICE LOCATION DATA

Additional Federal Actions Could Help Protect Consumer Privacy

What GAO Found

Using several methods of varying precision, mobile industry companies collect location data and use or share that data to provide users with location-based services, offer improved services, and increase revenue through targeted advertising. Location-based services provide consumers access to applications such as real-time navigation aids, access to free or reduced-cost mobile applications, and faster response from emergency services, among other potential benefits. However, the collection and sharing of location data also pose privacy risks. Specifically, privacy advocates said that consumers: (1) are generally unaware of how their location data are shared with and used by third parties; (2) could be subject to increased surveillance when location data are shared with law enforcement; and (3) could be at higher risk of identity theft or threats to personal safety when companies retain location data for long periods or share data with third parties that do not adequately protect them.

Industry associations and privacy advocates have developed recommended practices for companies to protect consumers' privacy while using mobile location data, but companies have not consistently implemented such practices. Recommended practices include clearly disclosing to consumers that a company is collecting location data and how it will use them, as well as identifying third parties that companies share location data with and the reasons for doing so. Companies GAO examined disclosed in their privacy policies that the companies were collecting consumers' location data, but did not clearly state how the companies were using these data or what third parties they may share them with. For example, some companies' policies stated they collected location data and listed uses for personal information, but did not state clearly whether companies considered location to be personal information. Furthermore, although policies stated that companies shared location data with third parties, they were sometimes vague about which types of companies these were and why they were sharing the data. Lacking clear information, consumers faced with making a decision about whether to allow companies to collect, use, and share data on their location would be unable to effectively judge whether the uses of their location data might violate their privacy.

Federal agencies have held educational outreach events, developed reports with recommendations aimed at protecting consumer privacy, and developed some guidance on certain aspects of mobile privacy. The Department of Commerce's National Telecommunications and Information Administration (NTIA) is implementing an administration-proposed effort to bring industry, advocacy, and government stakeholders together to develop codes of conduct for industry to address Internet consumer privacy issues generally. However, NTIA has not set specific goals, milestones, and performance measures for this effort. Consequently, it is unclear if or when the process would address mobile location privacy. Furthermore, the Federal Trade Commission (FTC) could enforce adherence to the codes if companies adopted them, but since adoption is voluntary, there is no guarantee companies would adopt the resulting codes. While FTC has issued some guidance to address mobile location privacy issues, it has not issued comprehensive guidance that could inform companies of the Commission's views on the appropriate actions companies should take to protect consumers' mobile location data privacy.

Contents

Letter		1
	Background	3
	Companies Collect, Use, and Share Location Data That Provide Consumer Benefits, but Also Pose Privacy Risks	9
	Private Sector Entities Have Not Consistently Implemented Recommended Practices to Protect Consumers' Location Privacy	19
	Federal Agencies Have Taken Actions to Protect Consumer Privacy, but Additional Actions Could Provide Further Protections	26
	Conclusions	36
	Recommendations for Executive Action	37
	Agency Comments and Our Evaluation	37
Appendix I	Objectives, Scope, and Methodology	40
Appendix II	Comments from the Department of Commerce	43
Appendix III	Comments from the Federal Trade Commission	46
Appendix IV	GAO Contacts and Staff Acknowledgments	51
Tables		
	Table 1: The OECD Fair Information Practices	7
	Table 2: Recommended Location Data Privacy Practices and Alignment with FIPs	20
	Table 3: Mobile Industry Companies We Examined	40
Figures		
	Figure 1: Roles of Mobile Industry Companies in Delivering Smartphone Functions	5
	Figure 2: Methods Used to Collect Location Information	11

Abbreviations

ACLU	American Civil Liberties Union
A-GPS	Assisted Global Positioning System
AMBER	America's Missing: Broadcast Emergency Response
Commerce	Department of Commerce
Communications Act	Communications Act of 1934
CPNI	customer proprietary network information
CTIA	CTIA-The Wireless Association
ECPA	Electronic Communications Privacy Act of 1986
E911	enhanced 911
FCC	Federal Communications Commission
FIP	Fair Information Practice
FTC	Federal Trade Commission
GPS	Global Positioning System
Justice	Department of Justice
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Co-operation and Development
Wi-Fi	wireless fidelity

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 11, 2012

The Honorable Al Franken
Chairman
Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

Dear Mr. Chairman:

The number of mobile phone subscriptions in the United States grew from about 3.5 million in 1989 to approximately 291 million by the end of 2009, according to the most recent Federal Communications Commission (FCC) data.¹ The Centers for Disease Control and Prevention reported that one-third of U.S. households had mobile phones but no landline phones as of December 2011.² Increasingly, Americans' mobile phones are smartphones, which use advanced operating systems to provide computing functions, including Internet access and a variety of applications, in addition to basic voice service. According to The Nielsen Company, as of June 2012, smartphones accounted for just over half of all mobile phones in the United States, up from less than one-quarter in early 2010.³

Smartphones allow users access to location-based services that can provide them with navigation tools and information relevant to their surroundings based on increasingly precise information about the user's

¹This estimate includes people with multiple subscriptions. Federal Communications Commission, *Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, Fifteenth Report (June 27, 2011).

²This estimate is based on a survey conducted by the Centers for Disease Control and Prevention's National Center for Health Statistics. The survey, which seeks to collect information on health issues, also includes questions about household telephones and whether anyone in the household has a wireless phone. S.J. Blumberg and J.V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey*, July-December 2011, a report for the Centers for Disease Control and Prevention, National Center for Health Statistics (June 2012). Available from: <http://www.cdc.gov/nchs/nhis.htm> (accessed July 11, 2012).

³The Nielsen Company, "Two Thirds of New Mobile Buyers Now Opting For Smartphones" (July 12, 2012).

current location determined by Global Positioning System (GPS) and other methods. Location-based services have proved popular with users; the Pew Research Center reported that three-quarters of smartphone users were using such services as of February 2012.⁴ In providing such services, smartphones and the companies that support their functions are able to collect and retain precise data about users' locations. Concerns have been raised about how mobile industry companies that provide or enable location-based services use and share consumers' location data, raising the potential that consumers' privacy could be violated if their location data are used in ways they did not intend or authorize.

Several agencies have responsibility to address mobile phone consumers' privacy and create related guidance. The Federal Trade Commission (FTC) has authority to take enforcement actions against unfair or deceptive acts or practices of companies; FCC has regulatory and enforcement authority over mobile carriers, such as AT&T and Verizon; 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 (Justice) disseminates guidance on procedures for law enforcement to request electronic evidence, such as a person's current or historical location data.

This report addresses

- (1) how mobile industry companies collect location data, why they use and share these data, and how this affects consumers;
- (2) the types of actions private sector entities have taken to protect consumers' privacy and ensure security of location data; and
- (3) the actions federal agencies have taken to protect consumer privacy and what additional federal efforts, if any, are needed.

To address these issues, we examined privacy policies and interviewed representatives from carriers, operating system developers, and smartphone manufacturers that are the largest in the United States by

⁴Kathryn Zickuhr, *Three-Quarters of Smartphone Owners Use Location-Based Services*, a report for Pew Research Center (Washington, D.C.: May 11, 2012).

market share and representatives from the developers of the most popular mobile applications on the Apple and Google operating systems.⁵ We reviewed documents and interviewed officials from FTC, FCC, NTIA, and Justice. We also interviewed privacy advocates and industry association representatives on their views. In considering ways to address location data privacy issues, we are reporting actions federal agencies could take, rather than potential legislative options. Recent proposals in Congress have sought to amend how the law treats mobile device location data, which is among the technology issues that have recently emerged.⁶ See appendix I for a more detailed description of our scope and methodology.⁷

We conducted this performance audit from December 2011 to September 2012 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

Smartphones combine the telecommunications functions of a mobile phone with the processing power of a computer, creating an Internet-connected mobile device capable of running a variety of software applications for productivity or leisure. The functioning of a mobile phone involves locating the user,⁸ and FCC's rules enabling enhanced 911 (E911) services require phones to provide GPS-quality location precision for emergency responders. This capability to determine a user's location has led to smartphones that can provide applications and services that

⁵Operating system developers are companies such as Apple, Google, and Research In Motion that develop the software that manages the hardware and applications of smartphones.

⁶See, e.g., Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); Electronic Communications Privacy Act Amendments of 2011, S. 1011, 112th Cong. (2011); Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011); Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011); and Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011).

⁷Concurrent with this review, we have examined mobile device security issues, including efforts by manufacturers, which is the subject of a separate report.

⁸A mobile carrier must know the location of a mobile phone to deliver incoming calls.

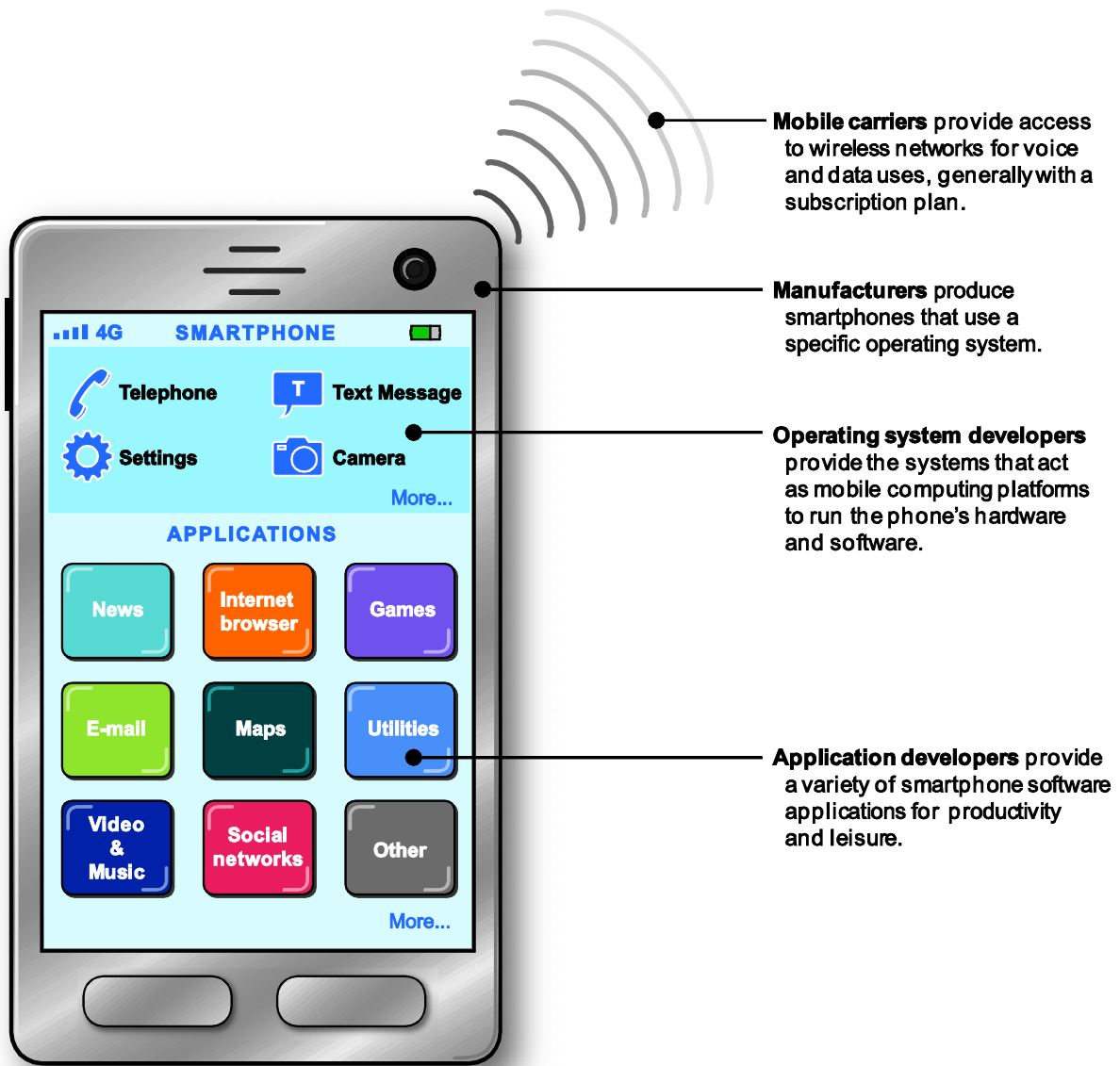
take advantage of location data generated by GPS and other location technologies. Advances in the technology for pinpointing a mobile phone's location have led to applications that identify a user's location quickly and with a high-level of precision.

Four types of companies are primarily responsible for smartphone products and services in the United States:

- Mobile carriers. Carriers provide smartphone users with access to wireless networks for voice and data uses, generally with a subscription plan. In the United States, four carriers primarily serve customers nationwide: AT&T, Sprint-Nextel, T-Mobile, and Verizon.
- Operating systems. Underlying the various functions of a smartphone is an operating system that acts as a mobile computing platform to run the phone's hardware and software. Three operating systems are most prevalent in the United States: Apple's iPhone iOS, Google's Android, and Research in Motion's BlackBerry.
- Manufacturers. Smartphones are made by a variety of electronics companies. Apple and Research in Motion manufacture phones based on their own proprietary operating systems. In contrast, a number of other companies, such as HTC, Motorola, and Samsung, make phones based on the Android operating system.
- Application developers. As the popularity of smartphones has grown, so too has the number of developers offering applications for them. New mobile applications are developed every day, with some estimates indicating there are more than a million available as of mid-2012. These developers range from start-up ventures to large, established Internet companies like Yahoo!, offering products like the Angry Birds game by Rovio Entertainment Ltd., social networking applications like Facebook, navigation tools like Google Maps, and music players such as Pandora Radio.

Together, the products and services developed by these various companies allow users to take advantage of the various functions smartphones provide (see figure 1).

Figure 1: Roles of Mobile Industry Companies in Delivering Smartphone Functions



Source: GAO.

Smartphones connect with mobile carrier networks for making calls and providing data services. Some smartphones also have the capability to connect with wireless fidelity (Wi-Fi) networks to provide data services.

Fair Information Practices

Fair Information Practices (FIP), are widely accepted principles for protecting the privacy and security of personal information. They were first proposed in 1973 by a U.S. government advisory committee. In response to concerns about the potential consequences that computerized data systems could have on the privacy of personal information, the committee was tasked to examine the extent to which limitations should be placed on using computer technology for record keeping about people.⁹ These principles, with some variation, have been used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States. FIPs are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other interests. Striking that balance varies among countries and among types of information (e.g., medical and employment information).

The Organisation for Economic Co-operation and Development (OECD), an international organization, developed a revised version of the FIPs in 1980 that has been widely adopted (see table 1).¹⁰

⁹See U.S. Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: July 1973).

¹⁰Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

Table 1: The OECD Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: OECD.

Laws that Govern Private-Sector Use of Personal Information

The Federal Trade Commission Act prohibits unfair or deceptive acts or practices affecting commerce and authorizes FTC enforcement action.¹¹ 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. FTC also enforces the Children's Online Privacy Protection Act of

¹¹An 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).

1998, which required FTC to promulgate rules governing the online collection of information from children under age 13.¹²

The Communications Act of 1934 (Communications Act), as amended, imposes a duty on mobile 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.¹³ The Communications Act requires express authorization for access to or disclosure of call location information concerning the user of commercial mobile services, subject to certain exceptions.¹⁴ Carriers must also comply with FCC rules implementing the E911 requirements of the Wireless Communications and Public Safety Act of 1999,¹⁵ including providing location information to emergency responders when mobile phone users dial 911.¹⁶

¹²Pub. L. No. 105-277, tit. XIII (Oct. 21, 1998, *codified at* 15 U.S.C. § §6501-6505). In response, FTC promulgated regulations implementing the Children's Online Privacy Protection Act of 1998. See 16 C.F.R. Part 312. Other laws FTC enforces that apply to specific industries could also be applicable to the extent that those companies make use of mobile location data. For example, the Gramm-Leach Bliley Financial Modernization Act requires the establishment of standards for regulated financial institutions to protect customers' privacy and safeguard their personal information, as well as disclose information-sharing practices to consumers and allow customers to limit the sharing of such information with third parties.

¹³CPNI 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).

¹⁴47 U.S.C. §222(f)(1).

¹⁵Pub. L. No. 106-81 (Oct. 26, 1999).

¹⁶47 C.F.R. § 20.18.

The Electronic Communications Privacy Act of 1986 (ECPA) sets out requirements under which the government can access information about a user's mobile phone and Internet communications.¹⁷ This includes legal procedures for obtaining court orders to acquire information relevant to a law enforcement inquiry.

Companies Collect, Use, and Share Location Data That Provide Consumer Benefits, but Also Pose Privacy Risks

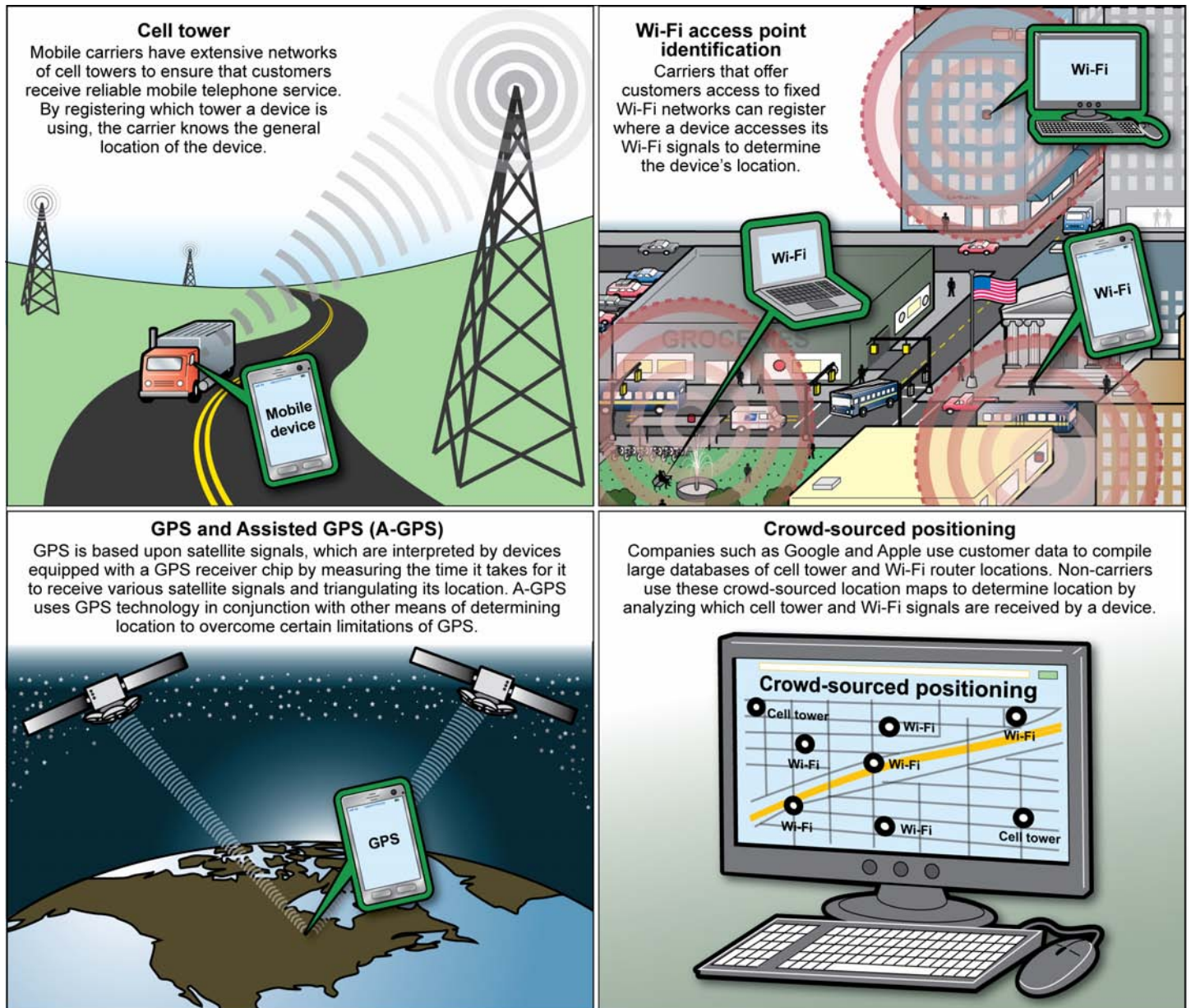
Collecting, using, and sharing location data provides benefits for both mobile industry companies and for consumers. For the companies, the main purposes for using and sharing location data are to provide and improve services, to increase advertising revenue, and to comply with legal requirements. Consumers, in turn, can benefit from these new and improved services and from targeted location-based advertising. Nonetheless, allowing companies to access location 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.

¹⁷Pub. L. No. 99-508 (Dec. 21, 1986).

**Companies Collect
Location Data in Various
Ways**

Mobile industry companies determine location information through various 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. Figure 2 below illustrates these technologies.

Figure 2: Methods Used to Collect Location Information



Source: GAO.

Cell Tower Signal-Based Technologies

Since the advent of consumer cellular technology, making and receiving mobile telephone calls has depended on the ability to determine a device's location from the constant radio communication between the device and the mobile carrier's cell towers that are spread throughout the

carrier's service area. The ranges of the individual cell towers divide the service area into separate sectors. As the towers are in fixed positions, determining a device's current cell tower sector tells the carrier the device's approximate location. The precision of this method depends on how much space a particular tower covers. In general, urban areas have smaller sectors than rural areas because each sector can only manage a certain amount of cell traffic at any one time. Because of increasing cell traffic, the number of cell towers has proliferated to the point that there are now over three times more than there were 10 years ago. As a result, cell sector-based location data are increasingly accurate. Companies can further improve accuracy by using triangulation methods, which determine location through the mathematical comparison of a device's signals that reach more than one cell tower. Cell tower triangulation can now yield results within 50 meters of accuracy.

Wi-Fi Access Point Identification

Mobile carriers that provide Wi-Fi access points to their customers can use these access points to determine location. Like cell towers, Wi-Fi access points are fixed locations and send out signals over a limited range. Specifically, Wi-Fi signals are radio waves that provide Internet access to devices equipped with compatible wireless hardware. Each Wi-Fi access point is identified by a unique hardware address. Nearby compatible devices are able to receive this information and use it to request Internet access. Since a Wi-Fi access point's range is limited to a few hundred meters, accurate location data can be determined if a device communicates with the access point.

Crowd-Sourced Positioning

Companies such as Google, Apple, and Skyhook use information gathered from users' mobile devices about cell tower and Wi-Fi access point signals, as well as the Wi-Fi signals of other companies and households, to determine location. These companies compile the precise locations of these signals into large databases, which the companies may then license to other entities such as application developers. An application installed on a mobile device can obtain location information by querying one of these databases, which will use its knowledge about those signals' locations to return the device's location. The database can also use location information sent by the device to update its records. If there are any new signals in the device's vicinity or any old signals that are no longer broadcasting, the database can incorporate those changes in its records. While the exact degree of accuracy ultimately depends on how many signal points are near the device when it queries a database, companies use crowd-sourced positioning because it provides accurate location data quickly, and because it does not rely on GPS technology, which is not available in all mobile devices.

GPS and A-GPS

GPS is used by both carriers and non-carriers to determine a device's location. GPS technology is based upon satellite signals, which are picked up and interpreted by devices equipped with GPS receiver chips. The device then measures the time it takes for it to receive various satellite signals and triangulates its location. Triangulating GPS satellite signals can yield data accurate to within 10 meters.

A-GPS is a hybrid approach used to overcome certain limitations in GPS technology: namely, that GPS usually only works outside buildings, may take several minutes to determine location, and uses more battery power than other location determination methods. By using GPS in conjunction with any of the previously described methods of collecting location data, the assisting technology can report an approximate location to the application or service while GPS works to obtain a more precise location. For instance, operating system and application developers may use crowd-sourced positioning databases to provide approximate locations to their users until GPS signals are successfully triangulated. The precision of A-GPS in these circumstances depends on the accuracy of the assisting method.

Mobile Industry Companies Use and Share Location Data for Various Reasons

There are three main reasons that mobile industry companies collect and share location data: 1) to provide and improve services, 2) to increase advertising revenue, and 3) to comply with court orders.

Provide and Improve Services

Mobile industry companies use location data to provide and improve services. As stated above, a carrier needs to know a device's location to provide basic mobile telephone services. In addition, carriers and application developers offer a diverse array of services that make use of location information, such as services providing navigation, the ability to keep track of family members, local weather forecasts, the ability to identify and locate nearby businesses, and social networking services that are linked to users' locations. To provide these services, carriers and developers need the ability 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 user'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 user 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.

Companies also collect and examine location information in conjunction with other diagnostic usage data to analyze and improve their interactions with customers. By examining the location patterns of dropped calls, for example, carriers can identify network problems and address cell connectivity issues without having to rely on customer complaints.

Furthermore, companies may use location data to provide public services. For example, carriers are responsible for providing law enforcement and other first responders with the location data of people who dial 911 from their mobile devices. This service is referred to as E911 and it is mandated by law.¹⁸ In addition, companies may provide location information to municipalities to improve city traffic management or facilitate city planning. Location data can also be used to help find missing children through mobile America's Missing: Broadcast Emergency Response (AMBER) alerts,¹⁹ which can be sent to devices that have requested AMBER alerts, when the devices are located within a specified radius of a reported incident.

Increase Advertising Revenue

Companies can use location data to target the advertising that users receive through mobile devices. Doing so may make an advertisement more relevant to a user than a non-targeted advertisement, boosting advertising revenue. Advertising is particularly important to application developers, as many developers give their products away free and rely on advertising for revenue. Advertisements for a certain business may be triggered if a user's device is located within a predetermined distance from that business. Any application, regardless of its function, may collect and use location data for advertising purposes.

Furthermore, application developers, operating system developers, and mobile carriers may aggregate and store individual user data to create user profiles. Profiles can be used to tailor marketing or service performance to an individual's preferences. In addition to capturing and using the location data of individual users, companies such as application developers and mobile carriers sell large amounts of de-identified location data to third parties. When data are de-identified, they are stripped of

¹⁸Pub. L. No. 106-81 (Oct. 26, 1999).

¹⁹The AMBER alert system broadcasts details about local child abductions over area television and radio stations, on highway signage, and, potentially, through other channels. The goal of the system is to enlist the public's help in child recovery efforts.

personally identifiable information.²⁰ In addition to de-identification, user data are often aggregated, which means that the data of many users are combined. Aggregation also makes it more difficult to distinguish the data of individuals. De-identified and aggregated data can be used for a variety of purposes, including marketing and research.

Comply with Court Orders

Mobile industry companies are legally required to share user location data in response to a court order if a court finds that the information is warranted for law enforcement purposes. Because users generally carry their mobile devices with them, law enforcement can use device location data to determine the user's location. Because of this correlation, location data are valuable to law enforcement for tracking the movements of criminal suspects. Of particular use are the location data either housed in mobile carrier databases or obtained through GPS technology. Mobile carriers are required to 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).

Location Data Use and Sharing Can Benefit Consumers, but Also Pose Privacy Risks

Many services that use location data were designed to make tasks easier or quicker for the customer, and the sharing of location data can improve customer experiences, reduce consumer costs, and help provide improved public services. Nonetheless, location data use and sharing may pose privacy risks, which include unknown third-party use, consumer tracking, identity theft, threats to personal safety, and surveillance.

Consumer Benefits

Consumers can benefit from mobile industry use of their location data because many location-based services are designed to make their lives easier and safer. For instance, navigation services enable users to easily find directions and take the guesswork out of finding the best or quickest routes, while applications designed to track family members enable parents to be aware of their children's whereabouts. An application may also use location data to personalize its usual services; for example, by using a location-aware business directory, a user may be able to rank search results by distance to save time and quickly reach the nearest location. Furthermore, as stated previously, the sharing of location data

²⁰Personally 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.

facilitates a faster response from emergency services through E911 and allows companies to identify network service problems.

Additionally, consumers may derive economic benefits from the sharing of their location data. For example, because many application developers depend on location-based advertising for revenue, users may be able to download applications for free or at a low cost. Furthermore, location-based advertising allows for targeted advertisements and offers to be sent to consumers, who may find them useful. For example, a user at lunchtime may receive and use a coupon for a local restaurant.

Consumer Privacy Risks

By allowing companies to access their location data, users expose themselves to privacy risks. These risks include, but are not limited to, disclosure to unknown third parties for unspecified uses, consumer tracking, identity theft, threats to physical safety, and surveillance.

Disclosure to Unknown Third Parties for Unspecified Uses

According to privacy advocates, when a user agrees to use a service that accesses location data, the user is unlikely to know how his or her location data may be used in ways beyond enabling the service itself. The secondary uses of location data are generally not transparent to the consumer.²¹ Therefore, location data may be shared with third parties unknown to the consumer. Generally speaking, once location data are shared with a non-carrier, consumers have a limited ability to know about or influence the data's use.

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. According to the congressional testimony of a privacy researcher,²² privacy notices rarely differentiate between first- and

²¹In the case of mobile carriers, the secondary usage of location data obtained for mobile telephone service is regulated by FCC's CPNI rules, which state that, unless a disclosure is required by law or approved by the customer, telecommunications companies may use, disclose, or permit access to CPNI in order to support their telecommunications services. 47 C.F.R. § 64.2005.

²²United States Senate, Judiciary Subcommittee on Privacy, Technology and the Law Hearing on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy, 112th Congress, page 8 (May 10, 2011) (testimony of Ashkan Soltani, Independent Researcher and Consultant).

third-party data uses and generally do not reveal specific business partners such as advertising networks, thus making it difficult for consumers to understand privacy risks. Because consumers do not know who these entities are or how they are using consumers' data, consumers may be unable to make meaningful choices and judge whether they are disclosing their data to trustworthy entities.

Tracking Consumer Behavior

When mobile location data are collected and shared, users may be tracked for marketing purposes without their consent. Since users 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 of an individual's activities. Amassing such data over time allows for the creation of a richly detailed profile of individual behavior, including habits, preferences, and routines—private information that could be exploited. Furthermore, since non-carriers' use of location data is unregulated, these companies do not have to disclose how they are using and sharing these profiles. 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 use is seen as contrary to consumers' expectations and results in unwanted solicitations or other nuisances.

Identity Theft

Identity theft occurs when someone uses another person's personal or financial information to commit fraud or other crimes. When sensitive information such as location data is disclosed, particularly when it is combined with other personal information, criminals can use this information to steal identities. 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 user'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 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

When mobile location data are collected and shared, users could be put at risk for personal threats if the data are intercepted by people who mean them harm. This is a potential concern for those people who do not want specific individuals to know where they are or how to find them, such as victims of domestic violence. 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 cause harm to the individual or his property through, for instance, stalking or theft. Access to location information also raises child safety concerns as more and more children access mobile devices and location-based services. According to the American Civil Liberties Union (ACLU), location updates that users 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 via 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.²³ For example, the ACLU reported in 2010 that Federal Bureau of Investigation agents investigating a series of bank robberies sought the records of every mobile phone that was near each bank when it was robbed. Furthermore, law enforcement agencies access location data frequently, access that could add to concerns about the potential for misuse. For example, in May 2012, Sprint-Nextel reported that it had received over 196,000 court orders for location information over the last 5 years.

Users 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

²³American Civil Liberties Union of Northern California. *Location-Based Services: Time for a Privacy Check-in* (San Francisco, Calif.: November 2010).

sensitive destinations, such as medical clinics, religious institutions, courts, political rallies, or union meetings.

**Private Sector
Entities Have Not
Consistently
Implemented
Recommended
Practices to Protect
Consumers' Location
Privacy**

Mobile industry associations and privacy advocacy organizations have recommended practices for industry to better protect consumers' privacy while making use of customers' personal information. Companies we examined have developed privacy policies to disclose information to consumers about the collection of location data and other personal information, but have not consistently or clearly disclosed to consumers what the companies are doing with these data or which third parties they may share them with.

**Recommended Practices
to Protect Privacy
Generally Align with FIPs**

Industry associations and privacy advocacy organizations have recommended practices for the mobile industry to better protect consumers' privacy while making use of their personal information. These recommended practices include actions to notify users about the collection and use of their location data, ways users can control data collection, safeguards for user data, and actions to demonstrate accountability. The recommended practices we identified generally align with the FIPs discussed earlier. For example, providing users with controls allowing them to opt in or opt out of having their location data collected aligns with the FIP principles of collection limitation, use limitation, and individual participation, since such controls allow users to limit the collection and use of their personal information while providing them greater ability to be informed about and control how their data are used. Specific examples of recommended practices are shown in table 2.

Table 2: Recommended Location Data Privacy Practices and Alignment with FIPs

Practice category	Examples of specific practices	Alignment with FIPs
Disclosures to users about data collection, use, and sharing	<ul style="list-style-type: none"> State reasons companies collect and share data. State specifically that collection of personal information is limited to specified needs. Data are not used for a purpose other than what has been disclosed to users without further notice and user consent. 	Purpose specification, openness, collection limitation, use limitation
User controls over location data	<ul style="list-style-type: none"> Obtain users' consent before collecting their personal information. Provide users the ability to opt out of data collection they have previously consented to. 	Collection limitation, use limitation, individual participation
Data retention and safeguards	<ul style="list-style-type: none"> State a specific time frame for retaining user data. Data should be protected with reasonable security safeguards against risks such as loss or unauthorized access. 	Purpose specification, security safeguards, use limitation
Accountability	<ul style="list-style-type: none"> Be responsible for protecting users' data. 	Accountability

Source: GAO analysis of practices recommended by industry and privacy advocacy organizations.

Companies Take Steps to Protect Privacy, but Not Consistently

Although companies we examined have taken steps to protect the privacy and security of location data, they have not done so consistently, and their actions sometimes fall short of the recommended practices we identified. The 14 mobile industry companies we examined reported actions to inform users about the collection, use, and sharing of their location data primarily through disclosures in their privacy policies.²⁴ Companies also disclosed information about ways consumers could control location data collection, how long companies retain location data, how companies safeguard the data, and companies' measures to demonstrate accountability, although how companies addressed these issues varied. While companies' disclosures routinely informed consumers that their location data were being collected, companies' disclosures did not consistently or clearly explain the purposes behind

²⁴We reviewed the privacy policies of the carriers, operating system developers, and application developers, which together represented 11 of the 14 companies. We did not review privacy policies for the three manufacturer companies. Some companies represented more than one type of company; for example, Apple is both an operating system developer (iPhone iOS) and manufacturer (iPhone). We sought interviews with all of the companies; 2 of them—Motorola and Samsung—provided written answers to our questions and a third, Apple, did not answer our questions but provided related documents in response to our request.

Data Collection, Use, and Sharing

such collection or identify which third parties these data might be shared with.

Recommended practices state that companies should clearly disclose to consumers the collection and use of location data and purpose for doing so. We found that while companies used privacy policies to inform users about location data collection, information about use and sharing was sometimes unclear. All 11 of the mobile carriers, operating system developers, and application developers we examined had privacy policies. Ten of the 11 privacy policies we examined disclosed that the company collected consumers' location data.²⁵ However, some policies were not clear about how the companies used location data. For example, the privacy policies of 4 of the companies we examined stated ways the companies used "personal information," but did not state whether location data were considered "personal information." It was therefore unclear whether these uses applied to location data. Companies' policies on whether location data were considered personal information varied. Apple's privacy policy, for example, stated that it considered location data to be nonpersonal information.²⁶ In contrast, T-Mobile's policy stated that location is personally identifiable information. Furthermore, representatives from four of the companies told us that whether location data is considered personal information depends on factors such as how precise the data are and whether they are combined with other information about the user.²⁷ The operating system developers

²⁵The privacy policy we examined from Research in Motion, the manufacturer and developer of the operating system for the BlackBerry mobile device, did not mention whether the company collects and uses location data. In a May 9, 2011, letter to Representative Fred Upton, Research in Motion described how BlackBerry devices may collect and use location data, which is explained in a licensing agreement that users must accept. Subsequently, in August 2012, Research in Motion released an updated privacy policy that states the company may collect and store location data associated with the use of location-based services. The policy explains that such data does not personally identify the user.

²⁶According to Apple's privacy policy, precise location data are collected anonymously in a form that does not personally identify the user. The policy also states that if Apple combines nonpersonal information with personal information, the combined information is treated as personal information. The policy does not state whether it is Apple's practice to combine location data specifically with personal information.

²⁷Four privacy policies stated or implied that personal information collected from users included location data; two policies made it clear that they did not consider location to be personal information; one policy indicated that it varied; and the remaining four policies did not state whether location data was considered personal information.

reported they collected location data in an anonymous manner or took steps to de-identify stored data. In contrast, 3 of the application developers we interviewed stated they stored location data with other personal information about their users.²⁸ Carriers told us that their practices varied, depending on the specific use of the data.

Recommended practices state that companies should inform consumers about third parties the companies share consumers' data with and the purposes for doing so. Most policies we examined stated the types of third-party companies location data may be shared with, such as application developers and advertisers; however, some policies described third parties with vague terms such as "trusted businesses" or "others." Although some policies stated that the company takes steps to protect this information, such as requiring the third party to follow the company's privacy policy, others made no such statement, and one company's policy said it would not be liable if the third party it shares data with fails to protect it. According to literature examining mobile applications, some applications lack privacy policies and consumers often do not know which companies may receive their personal information after it has been collected by the applications.²⁹

Companies also used other methods in addition to privacy policies to inform consumers about location data collection and use, including some methods that informed consumers directly through their phones. For example, some smartphone screens display an icon to indicate when location information is actively being used.

Controls

Recommended practices state that companies should obtain users' consent for collecting, using, and sharing personal information, including location data and explain related controls to users. Companies we contacted reported providing methods for users to control collection and

²⁸Two of the other application developers we interviewed told us their applications did not collect location data other than more general data collected during registration such as a user's ZIP code or country. Thus, discussion of whether location data are personally identifiable was not applicable to those companies.

²⁹The Future of Privacy Forum examined the ten most popular paid and free applications for three operating systems in September 2011 and found that about half of the applications had privacy policies, and a January 2011 TRUSTe analysis of the top 300 most popular free applications on those three operating systems found that 23 percent had privacy policies, while the others did not.

use of location data, but the methods and amount of control varied. Most of these companies indicated that users 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. While all of the operating system developers we examined allowed a user to have location access turned on or off for all applications, some gave users the ability to control whether specific applications could have access to location data. According to the literature we reviewed that examined mobile applications, controls within applications, if available, were sometimes difficult to find. Mobile carriers told us that they do not allow users to control collection of location data for providing basic phone service, since having location data is necessary to provide that service.

All the companies we examined that collected data for providing location-based services indicated that users must first provide consent before location-based services use their location; however, privacy policies we examined did not always explain how users' consent is obtained. Companies told us that a smartphone seeks permission from the user to use location when the user installs an application that makes use of location or the first time the user activates such an application. For example, the iPhone iOS operating system displays a pop-up window the first time a user activates a new application that includes location-based services. The pop-up states that the application is seeking to use the user's location and allows the user to accept or decline. Similarly, Android smartphones notify users that an application will use location at the time a user downloads a new application and seeks user consent through this process.

Retention and Safeguards

The recommended practices we reviewed state that companies should not keep personal information such as location data longer than needed, and some organizations encouraged companies to state a specific data retention time frame. However, 7 of the 11 privacy policies we reviewed did not include a statement about how long the company kept location data. Officials from most companies told us they kept location data only as long as needed for a specific purpose; however, in some cases, this could mean keeping location data indefinitely. The carriers we interviewed named specific time periods for location data retention, which they said varied depending on the specific uses of the data, and reported a range of time from a few days to 3 years after the duration of time a user is a customer with the company. Three companies indicated they kept location data indefinitely, and representatives from one company said they had not established a retention time period. Privacy advocates raised data retention as a particular concern, since the longer companies

retain location data, the more likely the potential for misuse. Similarly, FTC's March 2012 report on protecting consumers' private information stated that companies should delete location data as soon as possible, consistent with the services they provide to consumers.³⁰

Recommended practices consistently stated the need for companies to safeguard collected user data. Companies reported actions to safeguard users' location data, but practices for how data are safeguarded varied. All the companies we examined reported ways they safeguard users' personal information. For example, all of the privacy policies stated that companies had general security measures in place to protect personal information against loss, theft, or misuse. Specific practices reported by some companies included data encryption, erecting firewalls, and restricting employee access.³¹ In some cases, however, it was not clear whether these protections covered location data. As stated above, some privacy policies did not state whether location was considered a form of personal information, and thus it was unclear whether stated safeguards for personal information applied to location data.

Accountability

Most of the recommended practices expressed the need for companies to demonstrate accountability for their practices. However, companies' privacy policies reported few, if any, specific measures for accountability. Five of the 11 privacy policies included general statements that employees were accountable for following the company's policies as outlined in the privacy policy. A few privacy policies also mentioned that the company followed recommended practices; one carrier's policy stated the company followed recommended practices developed by CTIA-The Wireless Association (CTIA), a nonprofit organization representing mobile carriers and other wireless companies, and 3 companies' policies stated their privacy practices had been certified by TRUSTe, a company that helps companies address privacy issues. Three of the carriers also told us they use their contracts with third parties they share users' personal data with to require those third parties to adhere to CTIA recommended practices for location data. Operating system developers reported varying steps to encourage or require developers of applications that run on their

³⁰Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C.: March 2012).

³¹Manufacturers told us their phones include security features and controls to protect customers' personal information.

systems to inform users and obtain consent before using their location data. For example, in 2011, Apple stated that it would reject applications from its on-line store that do not obtain consent from the user before collecting, transmitting, or using a user's location data and that such use must be directly relevant to the features and services provided by the application. In contrast, Google stated that it does not control the behavior of third-party applications in handling location data, but encourages the developers to follow common privacy practices, such as giving users a choice regarding data collection and collecting only necessary information.

Inconsistent Practices to Protect Location Privacy Raise Risks

Companies' inconsistent adherence to recommended practices increases the likelihood that users could be exposed to the privacy risks we discussed previously. For example, because companies have not made clear and consistent disclosures about how they use and share location data, consumers may be unaware which third parties are using their location data (or that third parties are using it at all) and that law enforcement may obtain their location data and use it for surveillance. Furthermore, because consumers are expected to rely on these disclosures when judging whether they should give consent to a company to access their location, consumers may be providing such consent without complete knowledge of how their data will be used. For example, although privacy policies generally discussed that users' data could be shared with third parties, they sometimes included vague statements like "trusted business partners" rather than specifying the types of companies they shared the data with and the reasons for doing so. Consequently, users lack sufficient information to adequately judge whether they should trust those companies with their personal information.

Privacy advocates we spoke to acknowledged that companies have taken some positive steps to protect privacy, but that the current framework of self-regulation is exposing consumers to unnecessary risks. These advocates said that companies are generally disclosing to users that they will collect location data; however, they are not adequately informing consumers about the uses of the data they collect, including with whom they are sharing the data. These advocates also expressed concern about companies retaining location data longer than necessary, which puts the data at increased risk of inappropriate use. Furthermore, they told us the current framework of self-regulation is insufficient to address these concerns because there are no requirements for companies to consistently implement recommended practices to protect privacy.

Federal agencies that have examined location-based services have also noted that the benefits from such services come with concerns. For example, FCC, in its 2012 report on location-based services, noted that such services are expected to deliver \$700 billion in value to consumers and business users over the next decade.³² However, in summarizing views of participants in a 2011 panel discussion, the FCC report noted that panelists found inconsistency in the privacy notices provided by companies and incomplete disclosure of the ways location data are used. Specifically, the report states that while consumers may have clear notice that an application will collect and use data on their location, these data may be subsequently used in ways that are not transparent to consumers or shared with third parties without consumers' consent. FTC, in its report on protecting consumer privacy, noted that the unauthorized disclosure to third parties of sensitive personal information such as precise location data raises privacy concerns resulting from the unanticipated uses of these data.³³

Federal Agencies Have Taken Actions to Protect Consumer Privacy, but Additional Actions Could Provide Further Protections

Federal agencies that have responsibility for consumer privacy protection or that interact with the mobile industry have taken steps to promote public awareness, such as providing educational outreach and recommending actions aimed at improving consumer privacy. However, additional actions could be taken to further protect consumers. For example, NTIA has not defined performance goals 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. Additionally, FTC has not issued comprehensive guidance to mobile industry companies with regard to actions they should take to protect mobile location data privacy.

³²Federal Communications Commission, *Location-Based Services: An Overview of Opportunities and Other Considerations* (Washington, D.C.: May 25, 2012).

³³Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C.: March 2012).

Agencies Have Taken Actions to Promote Awareness of Privacy Issues

Several federal agencies that interact with the mobile industry or have responsibilities for consumer privacy protection have provided educational outreach to the public, developed reports with recommendations aimed at protecting consumer privacy, developed regulatory standards that address mobile-location data privacy, and developed guidance for law enforcement on obtaining mobile location data.

Educational Outreach

FCC and FTC have held educational outreach events, and FTC has developed a fact sheet to educate the public on various privacy issues related to location-based services. In June 2011, the agencies collaborated to hold a public education forum that explored how consumers can be both knowledgeable and secure when utilizing location-based services. Participants in the forum included representatives from mobile carriers, technology companies, consumer advocacy groups, and academia. Specific topics discussed included

- how location-based services work;
- trends, benefits, and risks of location-based services;
- industry recommended practices; and
- what parents should know about location tracking when their children use mobile devices.

Also in June 2011, FTC issued an informational fact sheet that provided basic information on mobile applications and answered questions on privacy, advertising, and security concerns.³⁴ Specific topics included the types of data that applications can access on users' devices, the reasons a user's phone collects location data, and ways that applications can cause harm to a user's phone.

In May 2012, FTC held a public workshop on advertising and privacy disclosures to discuss the need for new guidance for online advertisers about making disclosures. Participants included consumer advocates, representatives of industry groups, and academics. The workshop covered topics including

- when, where, and how required disclosures should be made;

³⁴The fact sheet is available at <http://onguardonline.gov/articles/0018-understanding-mobile-apps> (accessed Jan. 27, 2012).

-
- the techniques to increase or decrease the likelihood that consumers will actually read a required disclosure;
 - the challenges and best approaches to making adequate disclosures given the screen size constraints of mobile devices; and
 - the steps companies can take to communicate with consumers in a clear and consistent way about the companies' privacy practices.

In August 2012, FTC issued guidance for application developers to help developers comply with truth-in-advertising standards and basic privacy principles. The guidance discusses the need for developers to be clear to users about companies' practices to collect and share data, to offer users ways to control how their personal information is collected and shared, and the need to keep users' data secure, among other issues.³⁵

Reports on Consumer Privacy

Several agencies have issued or prepared reports that offered recommendations aimed at improving consumer privacy, including location-based services. In February 2012, NTIA prepared a report for the White House on protecting privacy and promoting innovation in the global digital economy.³⁶ 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. The report also urged Congress to pass consumer data privacy legislation that would, among other things, codify the consumer privacy bill of rights described in the report, grant FTC authority to enforce the bill of rights, and create a national standard under which companies must notify consumers of unauthorized disclosures of certain kinds of personal data.

Also in February 2012, FTC issued a report on privacy disclosures for mobile applications aimed at children.³⁷ 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

³⁵The guidance is available at <http://business.ftc.gov/documents/bus81-marketing-your-mobile-app> (accessed Aug. 20, 2012).

³⁶The 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).

³⁷Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Washington, D.C.: February 2012).

transparency about their data practices. The report recommended, among other things, that all companies that are involved in developing children's applications—the application stores, developers, and third parties providing services within the applications—should play an active role in providing key information to parents who download applications through simple, short disclosures that are easy to find and understand on the small screen of a mobile device.

In March 2012, FTC issued another report that laid out recommendations for businesses and policy makers aimed at protecting consumer privacy.³⁸ The report described recommended practices for companies that collect and use consumer data to develop and maintain processes and systems to implement privacy and data security practices. These practices include promoting consumer privacy at every stage of the development of products and services, and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency. The report also included recommendations to companies that make use of precise mobile location data, including that they should obtain affirmative express consent from consumers before collecting precise location data; limit collection to data needed for a requested service or transaction; establish standards that address data collection, transfer, use, and disposal, particularly for location data; and, to the extent that location data are collected and shared with third parties, work to provide consumers with more prominent notice and choices about such practices. The report also called on Congress to consider enacting baseline privacy legislation, reiterated FTC's call for legislation governing data security and data broker issues, and urged the industry to accelerate the pace of self-regulation.

Lastly, in May 2012, FCC issued a report that gave an overview of the opportunities and considerations of location-based services.³⁹ The report describes the value that location-based services may provide to the economy and consumers, challenges companies face as they attempt to provide consumers with appropriate notice and choice, steps the industry

³⁸Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C.: March 2012).

³⁹Federal Communications Commission, *Location-Based Services: An Overview of Opportunities and Other Considerations* (Washington, D.C.: May 25, 2012).

is taking to respond to these challenges, and new issues that continue to emerge in this area.

Regulatory Actions

There have been three relevant regulatory actions in the area of protecting mobile location data. In 1998, FCC, implementing requirements of section 222 of the Communications Act, as amended, developed rules to protect CPNI; subsequently, the law was amended to clarify that CPNI includes subscribers' call location data that carriers use to provide telecommunications services.⁴⁰ As previously discussed, FCC's regulations limit instances where CPNI can be used or disclosed without customer consent. In November 2000, CTIA proposed the adoption of location information privacy principles that covered the issues of notice, consent, security and integrity of information, and technology neutrality and urged FCC to conduct a rulemaking separate from its general CPNI proceeding, based on CTIA's assessment that the location privacy question is uniquely a wireless concern. In July 2002, FCC declined to initiate a rulemaking because it opined that the amendments to the Communications Act imposed protections for consumers, such as requiring express approval before carriers can use consumers' location information.⁴¹ The Commission decided that rules would be unnecessary and potentially counterproductive because of the still-developing market for location-based services and that CTIA's proposed privacy principles could be adopted by mobile industry companies on a voluntary basis.

In September 2011, FTC proposed amending its rule pertaining to the Children's Online Privacy Protection Act that would revise the definition of personal information to explicitly include location data.⁴² According to FTC

⁴⁰The Communications Act of 1934 requires telecommunications providers to secure customers' personal information identified as CPNI. The Wireless Communications and Public Safety Act of 1999 amended section 222 of the Communications Act to make clear that information on the location of customers when they make wireless calls is CPNI and impose specific obligations on carriers not to divulge location information without a customer's explicit consent. 47 U.S.C. § 222.

⁴¹Specifically, FCC found the amendments to the Communications Act requiring express prior authorization before using or disclosing location information were unambiguous and clearly imposed legal obligations. 47 U.S.C. § 222; FCC, *In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices*, FCC 02-208, WT Docket No. 01-72 (July 24, 2002).

⁴²The Children's Online Privacy Protection Act of 1998 required FTC to promulgate a rule governing the online collection of information from children under age 13.

officials, there is no time frame for the issuance of a final rule in this proceeding, as the Commission is still in the process of evaluating comments.⁴³

In June 2012, FCC solicited comments regarding the privacy and data security practices of mobile wireless service providers with respect to customer information stored on their users' mobile communications devices, which could include location information, and the application of existing privacy and security requirements to that information.⁴⁴ Since the Commission last solicited public input on this question 5 years ago and technologies and business practices in this area have changed, the Commission sought comments on a variety of issues including:

- the applicability and significance of telecommunications carriers' duty under section 222(a) of the Communications Act to protect customer information stored on their users' mobile communications devices;
- whether the definition of CPNI could apply to information collected at a carrier's direction even before it has been transmitted to the carrier;
- what factors are relevant to assessing a wireless provider's obligations under section 222 of the Communications Act, as amended, and the Commission's implementing rules, or other provisions of law within the Commission's jurisdiction, and in what ways;
- what privacy and security obligations should apply to customer information that service providers cause to be collected by and stored on mobile communications devices; and
- what should be the obligations when service providers use a third party to collect, store, host, or analyze such data.

⁴³76 Fed. Reg. 59804 (Sept. 27, 2011). In August 2012, FTC issued a supplemental notice of proposed rulemaking pertaining to the Children's Online Privacy Protection Act, 77 Fed. Reg. 46643 (Aug. 6, 2012).

⁴⁴77 Fed. Reg. 35336 (June 13, 2012).

Guidance for Law Enforcement
on Obtaining Mobile Location
Data

Justice has developed guidance on how law enforcement may obtain mobile location data,⁴⁵ which is primarily obtained through various court orders. These methods have been the subject of recent litigation. There are various methods in which mobile location data can be obtained, including, but not limited to:

- *Warrant*: A warrant allows law enforcement to obtain prospective mobile location data generated by GPS or similar technologies (i.e., where the device is currently located).⁴⁶ To obtain a warrant for these data, the government must establish probable cause to believe that the data sought will aid in a particular apprehension or conviction. This method requires the highest standard of evidence of all methods outlined below.
- *Section 2703(d) Court Order*: A 2703(d) court order allows law enforcement officials to obtain certain kinds of historical mobile location data (i.e., where the device was located in the past) that providers collect for business purposes.⁴⁷ To obtain this order, the government must offer specific and articulable facts showing that there are reasonable grounds to believe that the data are relevant and material to an ongoing criminal investigation.
- *Hybrid Order*: Justice has routinely acquired, since at least 2005, certain categories of prospective mobile location data generated by cell tower information through the combination of two court orders, the Pen/Trap court order⁴⁸ and the 2703(d) order. The combination order is known as a “hybrid order.” To obtain this order, law enforcement officials must affirm that the information likely to be obtained is relevant to an ongoing criminal investigation and further demonstrate specific and articulable facts showing that there are reasonable

⁴⁵See, 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).

⁴⁶FED. R. CRIM. P. 41.

⁴⁷18 U.S.C. §§ 2701-2712.

⁴⁸18 U.S.C. § 3121. The Pen Register and Trap and Trace Statute allows law enforcement to obtain prospective non-content information associated with communications.

grounds to believe that the information sought is relevant and material to an ongoing criminal investigation. This order is used because the Communications Assistance for Law Enforcement Act of 1994 precludes law enforcement officials from relying solely on the authority of the Pen/Trap statute to obtain cell tower data for a mobile customer.⁴⁹

- *Section 2702 Voluntary Disclosure:* Communications providers are permitted by law to voluntarily disclose information to law enforcement if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.⁵⁰

As already described, law enforcement agencies access location data frequently using these various authorities. Law enforcement's use of location information has spurred courts to review government actions to compel third parties to disclose location data, as judges question and examine what legal standards govern law enforcement access to historical and prospective location information.⁵¹ For example, in 2010, a federal district court in Texas denied government applications for historical cell site data, declaring that compelled warrantless disclosure of cell site data violates the Fourth Amendment.⁵² In contrast, in 2012, a federal district court in Maryland upheld the government's use of historical cell site data, concluding that the privacy issues surrounding the collection of historical cell site location records are best left for Congress to decide.⁵³

Concerns have been raised by privacy advocacy groups about the methods law enforcement can use to obtain location data. For example,

⁴⁹Pub. L. No. 103-414 (Oct. 25, 1994).

⁵⁰18 U.S.C. § 2702.

⁵¹Stephanie K. Pell and Christopher Soghoian, "Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact," *Berkeley Technology Law Journal*, vol. 27, no.1 (2012).

⁵²*In re U.S. Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010). As of our reporting date, an appeal is pending with the U.S. Court of Appeals for the Fifth Circuit.

⁵³*United States v. Graham*, ___ F. Supp.2d ___, 2012 WL 691531 (D. Md. 2012).

the ACLU has opined that existing privacy laws fail to provide adequate legal protections for the increasingly detailed information that is collected by location-based services about consumers' physical locations and that consumers, location-based service providers, and the government are thus acting in uncertain legal territory. Further, most of the privacy advocates we spoke to opined that the government should obtain a warrant based on probable cause of a crime before it tracks, prospectively or historically, the location of a mobile phone or other mobile communications device. This approach seeks to treat historical and prospective location information equally and would require law enforcement to meet a higher standard before obtaining access to any location data.⁵⁴

NTIA's Proposed Stakeholder Process Lacks Defined Performance Goals and an Adequate Enforcement Mechanism

Our Standards for Internal Control in the Federal Government,⁵⁵ in conjunction with the Government Performance and Results Act of 1993,⁵⁶ state that agencies should set performance goals with specific timelines and measures for program performance. These documents assert that in order to better articulate a results orientation, agencies should create a set of performance goals and measures that addresses important dimensions of performance. They also assert that agencies should use intermediate goals and measures to show progress or contribution to intended results, while including explanatory information on the goals and measures.

Following the February 2012 report on consumer privacy, NTIA began implementing a multistakeholder process, which includes, among other groups, individual companies, industry groups, privacy advocates, and consumer groups. The purpose of the process is to develop codes of conduct that implement the general privacy principles presented in the report and that would be enforceable by FTC if the codes are publicly and affirmatively adopted by mobile industry companies. NTIA believes that the proposed process can provide the flexibility, speed, and decentralization necessary to address policy challenges by facilitating participants' working together to find creative solutions. NTIA also stated

⁵⁴Pell and Soghoian, "Can You See Me Now?"

⁵⁵GAO, *Internal Control: Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

⁵⁶Pub. L. No. 103-62 (Aug. 3, 1993).

that another key advantage of the multistakeholder process is that it can produce solutions in a more timely fashion than a regulatory process.

NTIA officials stated that because they are in the beginning stages of defining what the overall process would entail, they could not provide specific information about procedures, deliverables, or time frames. The first session was held on July 12, 2012, and addressed how companies providing applications and interactive services for mobile devices can be transparent about how the companies handle personal data.

Officials stated that since the sessions will be driven by the stakeholders, they were unsure if the sessions would cover location data; however, in its comments responding to a draft of this report, NTIA stated that it appears likely stakeholders will address transparency of mobile location-based services based on the topic of conversation at the July meeting. NTIA officials said they planned to hold further discussion sessions, where stakeholders would meet to address distinct issues, but all of the topics have not yet been identified and would be based on recommendations from the stakeholders. Officials stated there is no defined timeline for the remaining discussion sessions or the development of the guiding principles, although in August 2012, NTIA indicated that seven meetings had been scheduled before the end of 2012. Lacking defined performance goals, milestones, and deliverables, it is unclear whether NTIA's multistakeholder process will establish an effective means for addressing mobile location data privacy issues.

NTIA officials stated that individual companies' compliance with the codes of conduct produced through the process would be voluntary and that it is uncertain that the process will yield company self-regulations or a third-party monitored code. If companies do not volunteer to follow any resulting principles, enforcement would depend on whether a company's failure to adhere to the agreed-upon practices could be considered an unfair practice. As such, the proposed process does not include any mechanism for enforcing compliance with the guiding principles that may be developed, and NTIA cannot offer any assurance that the results of the process will lead to significant adoption of these principles.

FTC has the authority to take legal action against a company that engages in unfair acts affecting commerce, such as companies engaging in unfair business practices that are likely to cause substantial injury to consumers, which are not reasonably avoidable by consumers themselves. FTC has begun to address mobile location issues by holding public workshops and by releasing a report that laid out recommendations

aimed at protecting consumer privacy. It has also developed some guidance for companies that collect, use, and share mobile location data, such as including recommendations on location data collection in its March 2012 consumer data privacy report, including recommendations on improving disclosures to parents about the collection and use of personal information by applications geared toward children in its February 2012 report on that subject, and issuing guidance for application developers regarding collection and use of location data in August 2012. While these various guidelines touch on a number of issues related to mobile location data privacy, FTC has not published comprehensive industry guidance on its views of appropriate actions by mobile companies with regard to privacy. Specifically, by publishing an industry guide for these companies, FTC could help clarify for mobile companies its views on the appropriate actions for protecting privacy of consumers' location data.⁵⁷ Doing so could help set expectations for industry on appropriate steps to protect consumers' privacy if the issue has not been adequately addressed through the development and adoption of industry codes or the enactment of legislation. Such guidance could also clarify for companies circumstances under which FTC might take enforcement action against unfair acts.

Conclusions

The use and sharing of mobile location data offer benefits to mobile industry companies and consumers, such as providing and improving services and increasing advertising revenue. Nonetheless, these activities can also pose several risks to privacy, including disclosing data to unknown third parties for unspecified uses, consumer tracking, identity theft, threats to personal safety, and surveillance. While mobile industry associations and privacy advocacy organizations have recommended practices for industry to better protect consumers' privacy while making use of customers' personal information, these practices are not mandatory for the companies to implement. Mobile industry companies we examined have inconsistently implemented these practices. In particular, the lack of clear disclosures to consumers about how their location data are used and shared means that consumers lack adequate information to provide informed consent about the use of these data.

⁵⁷According to FTC, its industry guides are administrative interpretations by the Commission of the laws it administers and may have application to any matter of fact or law and it may relate to the practices of a particular industry or to practices common to many unrelated industries.

Consumers are therefore unable to adequately judge whether the companies with which their data are shared are putting their privacy at risk.

A key federal effort to address these privacy risks is NTIA's planned multistakeholder process, which seeks to develop industry codes of conduct. However, NTIA has not defined the effort's performance goals, milestones, or deliverables. It is therefore unclear if this process will address the risks to privacy associated with the use and sharing of mobile location data. While NTIA recommended that FTC should be granted the authority to enforce any industry codes of conduct that are developed from the multistakeholder process, the current process relies on the industry's voluntary compliance with resulting codes of conduct before FTC could enforce the provisions. Regardless of what results from the multistakeholder process, FTC has authority to take action against companies that engage in unfair and deceptive practices. However, FTC has not issued comprehensive industry guidance establishing its views on the appropriate actions that mobile companies should take to protect consumers' mobile location data privacy. Without clearer expectations for how industry should address location privacy, consumers lack assurance that the aforementioned privacy risks will be sufficiently mitigated.

Recommendations for Executive Action

To address privacy risks associated with the use and sharing of mobile location data, we recommend that the Secretary of Commerce direct NTIA, in consultation with stakeholders in the multistakeholder process, to develop specific goals, time frames, and performance measures for the multistakeholder process to create industry codes of conduct.

To further protect consumer privacy, we recommend that the Chairman of FTC consider issuing industry guidance that establishes FTC's views of the appropriate actions by mobile companies with regard to protecting mobile location data privacy. In developing the guidance, FTC could consider inputs such as industry codes developed through the NTIA multistakeholder process, recommended practices from industry and privacy advocates, and practices implemented by mobile industry companies.

Agency Comments and Our Evaluation

We provided drafts of this report to Commerce, FCC, FTC, and Justice for comment. We also provided relevant portions of the draft to mobile industry companies for comment. We received technical clarifications from all of the agencies and some of the companies, which we

incorporated into the report as appropriate. FCC and Justice did not provide comments on the draft.

Commerce provided written comments on a draft of this report, which appear in appendix II. The department disagreed with our recommendation to develop specific goals, time frames, and performance measures for the multistakeholder process to create industry codes of conduct to address privacy risks associated with the use and sharing of mobile phone location data. Specifically, Commerce's letter stated that while NTIA worked with stakeholders to establish a framework that encourages meaningful progress, it is not the agency's role to dictate timelines and deliverables, and that to do so could be counterproductive. We continue to believe that setting goals and time frames for the process could provide stakeholders and consumers with better assurance that the process will indeed result in the timely creation of industry codes to address privacy issues, as called for in the report on consumer privacy that NTIA prepared and that was released by the White House in February 2012. Furthermore, in its letter, Commerce acknowledged NTIA's role in setting a date and selecting a topic for the first multistakeholder process convened in July 2012 and a second process planned to begin in the fall. Thus, we believe it is reasonable to suggest that within its role to initiate and facilitate these meetings, NTIA could work with stakeholders to prioritize consideration of mobile phone location data privacy so that this issue, which, as we previously discussed, has been identified as a particular area of concern by privacy advocates and government agencies, is addressed in a timely manner. We have also revised the wording of the recommendation to state that NTIA's efforts should be done in consultation with the appropriate stakeholders involved in the multistakeholder process to develop industry codes of conduct.

FTC provided written comments on a draft of this report, which appear in appendix III. In its letter, FTC stated that it agreed that additional guidance for industry on mobile location data practices would be useful and stated that the agency will continue efforts to inform and guide the industry on best practices for mobile location data. However, FTC also raised concerns with our draft recommendation calling for such guidance to help inform mobile companies how FTC would enforce the prohibition against unfair acts pursuant to the Commission's authority under the Federal Trade Commission Act to take enforcement action against a company that engages in unfair acts affecting commerce. FTC stated that what constitutes unfair facts or practices is determined by statute and the test for determining what is an unfair practice is inherently fact specific in an area in which technology is changing rapidly. It concluded, therefore,

that its business guidance efforts may not necessarily be tied to determinations of what is unfair. Consequently, we modified the wording of our recommendation to FTC to focus on the need for FTC to clarify for mobile industry companies its views on appropriate actions companies should take to protect mobile location data privacy.

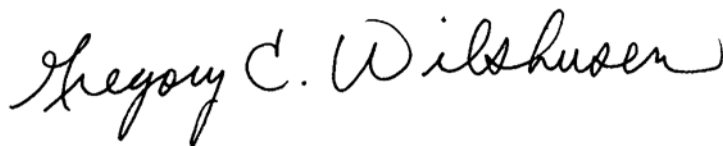
As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the relevant agencies. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov, or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,



Mark L. Goldstein
Director, Physical Infrastructure



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to examine

- (1) how mobile industry companies collect location data, why they use and share these data, and how this affects consumers;
- (2) the types of actions private sector entities have taken to protect consumers' privacy and ensure security of location data; and
- (3) the actions federal agencies have taken to protect consumer privacy and what additional federal efforts, if any, are needed.

To address all of the objectives, we examined the practices of mobile industry companies involved in the collection and use of location data; specifically mobile carriers, operating system developers, smartphone manufacturers, and application developers. We selected the carriers, operating system developers, and manufacturers with the largest market shares in the United States and the application developers using data on the most popular applications for the two operating systems with the largest market share, Apple iOS and Google Android. See table 3 below for a list of the companies we examined.

Table 3: Mobile Industry Companies We Examined

Type of company	Company names
Mobile carrier	AT&T, Sprint-Nextel, T-Mobile, Verizon
Operating system developer (name of system)	Apple (iPhone iOS), Google (Android), Research in Motion (BlackBerry)
Smartphone manufacturer	Apple, HTC, Motorola, Research in Motion, Samsung
Application developer (sample applications)	Facebook, Google (Gmail, Maps, News and Weather, Search, Talk, YouTube), Pandora (Radio), Rovio Entertainment Ltd. (Angry Birds), Yahoo! (Weather, Messenger)

Source: GAO.

We reviewed and analyzed selected companies' privacy policies and other publicly available documents. We also interviewed representatives of these companies, except Motorola and Samsung, which provided written answers to our questions, and Apple, which declined to answer our questions.

To address our first objective, we reviewed and analyzed relevant literature to determine the various methods companies use to collect

location data, why they use and share these data, the benefits that are provided to the consumer, and the associated privacy risks. In addition, we interviewed representatives from mobile industry associations (CTIA – The Wireless Association and Mobile Marketing Association), privacy advocacy groups (American Civil Liberties Union, Center for Democracy and Technology, Electronic Frontier Foundation, Electronic Privacy Information Center, and Future of Privacy Forum), and two privacy researchers (Christopher Soghoian and Ashkan Soltani) who had either testified on the subject before Congress or authored relevant literature on the subject, to discuss the benefits and privacy risks associated with the use of location data. We also interviewed officials from federal agencies that interact with the mobile industry or have responsibilities for consumer privacy protection, including the Federal Communications Commission (FCC), Federal Trade Commission (FTC), Department of Commerce’s National Telecommunications and Information Administration (NTIA), and Department of Justice (Justice), to obtain their views.

To address our second objective, in addition to examining the companies as previously discussed, we identified practices recommended by mobile industry associations and privacy advocacy groups to protect the privacy of and secure users’ personal information and assessed the extent to which they are consistent with the Fair Information Practices. In addition, we reviewed and analyzed the privacy policies of the selected mobile industry companies to determine their specific practices to protect consumer privacy and how their stated practices aligned with recommended practices. We also reviewed relevant studies of mobile application privacy to obtain further information on how mobile application developers protect consumer privacy. We also interviewed representatives of privacy advocacy groups to obtain their views about how the private sector is protecting users’ location privacy.

To address our third objective, we identified and reviewed relevant laws applicable to the mobile industry’s use of personal information. To evaluate how federal agencies have ensured compliance with relevant laws and what additional efforts they could take to further protect consumers, we analyzed information and interviewed officials from FCC, FTC, NTIA, and Justice about their enforcement, regulatory, and policymaking efforts to protect consumer privacy. We also interviewed representatives from mobile industry associations and privacy advocacy groups as well as privacy researchers to obtain their views about whether more could be done to protect consumer privacy. In considering ways to address location data privacy issues, we are reporting actions federal agencies could take, rather than potential legislative options.

We conducted this performance audit from December 2011 to September 2012, 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.

Appendix II: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

August 17, 2012

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Comptroller General Dodaro:

Thank you for the opportunity to comment on the Government Accountability Office (GAO) draft report entitled, *Mobile Phone Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, GAO 12-903. Staff from the National Telecommunications and Information Administration (NTIA) provided technical and editorial comments to the draft report on April 12, 2012; June 25, 2012; and August 8, 2012.

The report discusses how mobile industry companies collect and use consumers' location data and provides a valuable contribution to the understanding of mobile communications privacy practices. The report also raises concerns that the codes of conduct developed through the privacy multistakeholder process are voluntary and recommends that NTIA develop specific goals, timeframes, and performance measures for the multistakeholder process to create industry codes of conduct. However, for the reasons described in this letter, I respectfully disagree with your recommendation that I direct NTIA to develop specific goals, timeframes, and performance measures for the creation of codes of conduct.

While preparing the report, GAO met with officials from NTIA, the principal advisor to the President on telecommunications and information matters, including Internet policy. The Administration's comprehensive Blueprint to improve consumers' privacy protections in the information age assigns NTIA a leading role in advancing consumer privacy protections.¹ The Blueprint includes the Consumer Privacy Bill of Rights, which sets forth basic principles for consumers on what they should expect from those who handle their personal information and sets expectations for companies that use personal data. The Blueprint tasks NTIA with convening interested stakeholders to develop enforceable codes of conduct that specify how the principles in the Consumer Privacy Bill of Rights apply in specific business contexts.

¹ The Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, Feb. 23, 2012, available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (Blueprint).

The Honorable Gene L. Dodaro
Page 2

The Blueprint envisions that the codes will be voluntary, but, once adopted, they will be enforced by the Federal Trade Commission (FTC). The Blueprint calls for multistakeholder processes to develop the codes. Under this plan, the government provides the venue and the opportunity for discussion, but the stakeholders themselves—including industry, the public interest sector, and academia—drive the discussions towards consensus.

In implementing this model to develop initial privacy codes of conduct, NTIA worked with stakeholders to establish a framework that encourages meaningful progress, but it is not the role of NTIA to dictate timelines and deliverables; indeed, such an approach could be destructive to the multistakeholder process. However, NTIA anticipates that stakeholders will develop specific goals, set timeframes, and define deliverables as the multistakeholder process moves forward. This stakeholder-driven decision-making is consistent with the multistakeholder approach successfully and widely used around the world.

The multistakeholder approach has a particular history of success in addressing Internet-related issues. Organizations like the Internet Society, the Internet Engineering Task Force, and the World Wide Web Consortium have, for decades, led development of Internet technical standards and governance policies through broad-based, multistakeholder processes. Many of the technologies we take for granted when using the Internet, from the routing and addressing protocols that enable packet-switched networks to the HTML format behind every Web page, were developed with the participation and consensus of technology companies, academics, and other interest groups. The Internet Corporation for Assigned Names and Numbers, with which NTIA contracts to run the global system of assigning domain names and Internet Protocol addresses, makes its policy decisions through a multistakeholder process. The Organisation for Economic Co-operation and Development employs and recommends a multistakeholder approach for Internet policymaking. Based on the long-established effectiveness of the multistakeholder approach in supporting Internet innovation and defining meaningful privacy protections, NTIA will continue to use the multistakeholder approach to enhance consumers' privacy.

In the development of the Administration's Privacy Blueprint, the Department of Commerce has worked closely with the Federal Trade Commission (FTC) as the Nation's chief privacy enforcer. The FTC has indicated that it will look favorably on companies that subscribe to codes of conduct developed in the multistakeholder process. The Administration supports legislation that would strengthen enforcement of codes of conduct by giving the FTC direct authority to enforce the Privacy Bill of Rights and to grant safe harbors from enforcement for compliance with codes of conduct in implementing the Bill of Rights.

The Honorable Gene L. Dodaro
Page 3


On July 12, 2012, NTIA hosted the first multistakeholder meeting for consumer privacy, and scheduled seven additional meetings before the end of 2012. The topic of this first effort is the transparency of mobile applications—what information should be made available to users about how applications and service providers collect and use consumers' data. The meeting was a successful start to what will likely be an extended discussion of mobile transparency issues, and based on the first meeting, it appears likely that the stakeholder group will address the transparency of location services in the mobile app context.

NTIA will also take steps to begin a second consumer privacy multistakeholder process this fall. We have received a broad range of suggestions for topics for further privacy codes of conduct, and mobile location (beyond transparency) is certainly one of the topics under consideration. NTIA will select a topic based on its best judgment of both how to best advance consumer privacy and how to further establish the multistakeholder process as an effective means to develop privacy codes of conduct.

With respect to the GAO draft report's concerns about enforcement and the voluntary nature of the codes of conduct, we believe that the multi-pronged approach outlined by the Consumer Privacy Blueprint is best because it adequately balances the need to protect consumers while continuing to promote innovation on the Internet.

Thank you again for the opportunity to share our comments on this draft report. Please be assured that NTIA will continue to vigorously pursue the goal of enforceable codes of conduct to address consumer privacy concerns and such efforts will address at least some aspects of location privacy. The Administration is committed to enhancing online consumer privacy and will continue to work for legislation that advances this goal.

Sincerely,



Rebecca M. Blank
Acting Secretary of Commerce

Appendix III: Comments from the Federal Trade Commission



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

August 17, 2012

Mr. Mark L. Goldstein
Director, Physical Infrastructure Issues
United States Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Mr. Gregory C. Wilshusen
Director, Information Security Services
United States Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Messrs. Goldstein and Wilshusen:

On July 26, 2012, the Government Accountability Office (“GAO”) forwarded for the Federal Trade Commission’s (“FTC” or “Commission”) review and comment a draft of a GAO report entitled *MOBILE PHONE LOCATION DATA: Additional Federal Actions Could Help Protect Consumer Privacy* (GAO-12-903) (“draft report”). The draft report recommends that the Chairman of the FTC consider issuing industry guidance establishing the FTC’s views of appropriate actions by mobile companies with regard to protecting mobile location data privacy. This letter responds to GAO’s recommendation.¹

The Commission appreciates GAO’s careful and thorough assessment of the consumer privacy considerations regarding mobile phone location data. The Commission is pleased to have been able to assist GAO in conducting this assessment and welcomes the opportunity to comment on its draft report. The Commission shares a number of the concerns that GAO identified in its draft report about the consumer privacy risks associated with mobile location data, including the lack of transparency surrounding how such data is used and shared. For example, the Commission agrees with GAO that some companies “have not consistently or clearly disclosed to consumers what the companies are doing with [location] data or which third

¹ The Commission vote on this letter was 4-0-1, with Commissioner J. Thomas Rosch not participating.

parties they may share them with.”² Similarly, we agree that inadequate or inconsistent disclosures may mean that consumers may be providing consent to the use of location information “without complete knowledge of how their data will be used.”³

In response to GAO’s request that we issue guidance to companies with respect to mobile location data practices, the FTC notes that it has worked actively to provide such guidance in recent years. For instance, the FTC has developed and disseminated consumer and business education materials,⁴ hosted public workshops and outreach events,⁵ released reports,⁶ proposed to amend the Children’s Online Privacy Protection Act to affirm that location data is considered personal information under the Act,⁷ and testified twice before the current Congress on mobile location data.⁸ In addition to the Commission’s law enforcement in the privacy sphere, the FTC will continue its active efforts to provide guidance about data privacy practices, including those concerning location information, to companies operating in the mobile environment.

² See GAO, *MOBILE PHONE LOCATION DATA: Additional Federal Actions Could Help Protect Consumer Privacy* (July 2012), at 23.

³ *Id.* at 31.

⁴ See, e.g., FTC, *Understanding Mobile Apps* (Sept. 2011), available at <http://onguardonline.gov/articles/0018-understanding-mobile-apps>; FTC, *Marketing Your Mobile App: Get It Right From the Start* (Aug. 2012), available at <http://business.ftc.gov/documents/bus81-marketing-your-mobile-app>.

⁵ See, e.g., FTC Workshop, *In Short: Advertising & Privacy Disclosures in a Digital World* (May 30, 2012), available at <http://ftc.gov/bcp/workshops/inshort/index.shtml>; FTC Workshop, *Paper, Plastic...or Mobile? An FTC Workshop on Mobile Payments* (Apr. 26, 2012), available at <http://www.ftc.gov/bcp/workshops/mobilepayments/>.

⁶ See FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), available at http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; FTC, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, (Mar. 2012), available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

⁷ See *FTC Children’s Online Privacy Protection Rule*, 76 Fed. Reg. 59804 (proposed Sept. 27, 2011), available at <http://www.ftc.gov/os/2011/09/110915coppa.pdf>.

⁸ *Consumer Privacy and Protection in the Mobile Marketplace: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (2011) (statement of David C. Vladeck); *Protecting Mobile Privacy: Your SmartPhones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. for Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2011) (statement of Jessica Rich).

Highlighting a few of the most significant activities in greater detail, the Commission issued in March 2012 a report entitled *Protecting Consumer Privacy in an Era of Rapid Change* (“Privacy Report”), which offers guidance on appropriate actions by mobile companies with respect to protecting mobile location data privacy.⁹ The Commission’s Privacy Report raised, among other things, the potential for mobile devices to collect and retain location data that could be used to build detailed profiles of consumer movements over time and in ways not anticipated by consumers. The Privacy Report noted that these profiles could reveal a predictive pattern of the consumer’s movements, thereby exposing the consumer to a risk of harm such as stalking. Accordingly, the Commission called on companies to (1) obtain affirmative express consent from consumers before collecting precise geolocation data; (2) limit collection to data they need for a requested service or transaction (e.g., a wallpaper application (“app”) or an app that tracks stock quotes does not need to collect location information), (3) establish standards that address data collection, transfer, use, and disposal, particularly for location data, and (4) provide consumers with prominent notice and choices where location data is collected and shared with third parties.

The Privacy Report followed the release of a February 2012 FTC staff report on mobile apps for children that contained recommendations for all members of the children’s app ecosystem about conveying key information, such as the collection of location data, to parents.¹⁰ This report discussed a survey of 400 apps that were directed to kids and were offered through the two leading mobile platforms. With the survey, staff sought to determine what privacy disclosures were made available to consumers prior to downloading the apps. The report noted that companies offered very little information about their privacy practices and recommended that “all members of the kids app ecosystem – the app stores, developers, and third parties providing services within the apps – should play an active role in providing key information to parents who download apps.”¹¹ The report also encouraged app developers to provide information about data practices simply and succinctly.¹²

⁹ FTC, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, *supra* note 6.

¹⁰ See FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, *supra* note 6.

¹¹ *Id.* at 3.

¹² *Id.*

An FTC workshop in May 2012 also addressed innovative ways to improve mobile privacy disclosures to make them short, effective, and accessible to consumers.¹³ Based on the workshop record, including comments received after the workshop, FTC staff expects to issue a report on mobile privacy disclosures that will provide further guidance to companies in the mobile ecosystem to improve the transparency of their data practices, including their collection and use of location information.

Most recently, the FTC published educational materials offering guidance to help mobile app developers comply with truth-in-advertising standards and basic privacy principles, including how to handle location data.¹⁴ These materials advised companies, among other things, to “[e]xplain what information your app collects from users or their devices and what you do with their data” and “get users’ affirmative OK before you collect any sensitive data from them, like medical, financial, or precise geolocation information.”¹⁵ This publication has been made widely available in hard copy and through the FTC’s home page, the FTC’s Bureau of Consumer Protection Business Center website, the Bureau of Consumer Protection Business Center blog, the Commission’s Twitter feed, the FTC’s Facebook page, and OnGuardOnline.gov.¹⁶

In addition to issuing written materials, we have also actively worked to educate mobile companies directly. For example, staff members have spoken at numerous meetings of mobile app developers to advise them of the recommendations in our privacy report and to urge them to move forward on their efforts to improve transparency and address consumer privacy issues.¹⁷ Further, one of the Commission’s privacy experts is now located in our San Francisco Regional Office which permits more extensive outreach to the technology community on the West Coast.

¹³ See FTC workshop, *In Short: Advertising & Privacy Disclosures in a Digital World*, *supra* note 5.

¹⁴ See FTC, *Marketing Your Mobile App*, *supra* note 4.

¹⁵ *Id.*

¹⁶ OnGuardOnline is the federal government’s website to help consumers and business stay safe, secure, and responsible online.

¹⁷ For example, FTC staff has spoken at three regional Privacy Summits (in Austin, Texas, New York, New York, and Chicago, Illinois) for the Application Developers Alliance, as well as the West Coast App Developer Privacy Summit in Palo Alto, California, an event hosted by the Future of Privacy Forum, the Application Developers Alliance, and the Stanford Law School Center for Internet and Society. FTC staff has spoken at a number of other industry events as well.

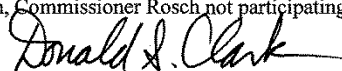
Finally, we have supported NTIA's efforts to convene various stakeholders in order to develop a code of conduct for mobile transparency. We attended the first multi-stakeholder meeting on this subject and will continue to monitor the process. We hope that this effort will yield a code of conduct that addresses the concerns that GAO identified in its report regarding mobile location data practices.

These activities underscore the Commission's belief that strong privacy and data security protections for consumers are critical for mobile location data. Although we believe the guidance we have offered to businesses on mobile location data practices is extensive, we agree that additional guidance can be useful and intend to continue our efforts to inform and guide industry on best practices for mobile location data.

With respect to GAO's recommendation that the guidance we provide be used to determine whether certain practices are unfair under the FTC Act,¹⁸ we note that our determination of what constitutes unfair acts or practices is determined by the statute. An unfair practice is one that caused or is likely to cause substantial consumer injury that is not reasonably avoidable and not outweighed by countervailing benefits to consumers or competition.¹⁹ In this area, the test is inherently a fact-specific one, which involves a weighing of costs and benefits that could result in a different analysis over time, as a result of rapid changes in technology in this area. For these reasons, our business guidance efforts with respect to geolocation information – while providing an important education function to companies in developing best practices – may not necessarily be tied to determinations of what is unfair.

The Commission again would like to reiterate its appreciation for GAO's thoughtful and careful examination of this issue and for the opportunity to respond to the recommendation in its report.

By direction of the Commission, Commissioner Rosch not participating.


Donald S. Clark
Secretary

¹⁸ See GAO draft report, *supra* note 2, at 44.

¹⁹ 15 U.S.C. § 45(n).

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Mark L. Goldstein (202) 512-2834 or goldsteinm@gao.gov

Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Michael Clements (Assistant Director), John de Ferrari (Assistant Director), Russell Burnett, Mark Canter, Marisol Cruz, Colin Fallon, Andrew Huddleston, Josh Ormond, David Plocher, Meredith Raymond, and Crystal Wesco made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

