



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

December 2013

IN-CAR LOCATION- BASED SERVICES

Companies Are
Taking Steps to
Protect Privacy, but
Some Risks May Not
Be Clear to
Consumers

GAO Highlights

Highlights of [GAO-14-81](#), a report to the Chairman, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

The prevalence of in-car communication systems provided by auto manufacturers (called telematics systems), PNDs, and smart phones has brought significant opportunities for consumers to access location-based services in their cars. As in-car location-based services have become commonplace, privacy groups and policy makers have questioned whether location data collected by companies can be used for purposes beyond the provision of services, such as by data brokers who collect information to resell the information.

GAO was asked to review this issue. This report addresses (1) what selected companies that provide in-car location-based services use location data for and if they share the data, and (2) how these companies' policies and reported practices align with industry-recommended privacy practices. GAO selected a non-generalizable sample of 10 companies. The companies were selected because they represent the largest U.S. market share or because their services are widely used. GAO examined documentation and interviewed representatives from each company regarding their privacy practices in effect in 2013 and compared those practices to industry recommended privacy practices.

What GAO Recommends

Since this report examines private companies' use of location data, GAO is not making recommendations to federal agencies. The Department of Commerce, Federal Trade Commission, and the selected companies provided technical comments, which GAO incorporated as appropriate.

View [GAO-14-81](#). For more information, contact Lori Rectanus at (202) 512-2834 or rectanusl@gao.gov.

December 2013

IN-CAR LOCATION-BASED SERVICES

Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers

What GAO Found

Representatives from all 10 selected companies—auto manufacturers, portable navigation device (PND) companies, and developers of map and navigation applications for mobile devices—said they collect location data to provide consumers with location-based services. For example, companies collect location data to provide turn-by-turn directions. Nine companies share location data with third-party companies, such as traffic information providers, to provide services to consumers. Representatives from two companies said they share data where personally identifiable information has been removed (de-identified data) for purposes beyond providing services (e.g., for research), although such purposes are not always disclosed to consumers. All company representatives said that they do not share personally identifiable location data with or sell such data to marketing companies or data brokers.

All 10 selected companies have taken steps consistent with some, but not all, industry-recommended privacy practices. In addition, the companies' privacy practices were, in certain instances, unclear, which could make it difficult for consumers to understand the privacy risks that may exist.

- **Disclosures:** Consistent with recommended practices, all selected companies disclose that they collect and share location data. However, inconsistent with recommended practices, nine companies' disclosures provide reasons for collecting data that are broadly worded (e.g., the stated reasons for collecting location data were not exhaustive), and five companies' disclosures do not describe the purposes for sharing de-identified location data. Without clear disclosures, risks increase that data may be collected or shared for purposes that the consumer is not expecting or might not have agreed to.
- **Consent and controls:** Consistent with recommended practices, all selected companies obtain consumer consent to collect location data and obtain this consent in various ways. In addition, all companies offered consumers some controls over location data collection. However, if companies retained data, they did not allow consumers to request that their data be deleted, which is a recommended practice. Without the ability to delete data, consumers are unable to prevent the use or retention of their data, should they wish to do so.
- **Safeguards and retention:** All selected companies take steps to safeguard location data—a recommended practice—but use different de-identification methods that affect the extent to which consumers may be re-identified and exposed to privacy risks. Also, there is wide variation in how long companies retain vehicle-specific or personally identifiable location data. To the extent that a company's de-identification methods allow a consumer to be identified or that identifiable data are retained, risks increase that location data may be used in ways consumers did not intend or may be vulnerable to unauthorized access.
- **Accountability:** All selected companies disclose to consumers or take steps to protect location data that they share with third parties; such efforts are consistent with recommended practices. However, inconsistent with recommended practices, none of the selected companies disclose to consumers how they hold themselves and their employees accountable. The companies told GAO that internal company policies serve this function.

Contents

Letter		1
	Background	4
	Selected Companies Stated That They Primarily Collect and Share Location Data to Provide and Improve Consumer Services	9
	Selected Companies Have Implemented Some Recommended Practices, but the Extent to Which Consumers' Privacy Could Be at Risk May Not Be Clear	12
	Agency Comments	21
Appendix I	Objectives, Scope, and Methodology	23
Appendix II	GAO Contact and Staff Acknowledgments	27
Tables		
	Table 1: Industry-Developed Recommended Privacy Practices Applicable to Location Data	6
	Table 2: Select Laws That Address Consumer Privacy and Their Relevance to Privacy of Location Data	7
	Table 3: Selected Companies That Provide In-Car Location-Based Services	23
Figures		
	Figure 1: Description and Examples of Systems or Devices That Deliver In-Car Location-Based Services to Consumers	4
	Figure 2: How Location Data Are Transmitted to Provide In-Car Location-Based Services	5
	Figure 3: Examples of De-Identification Methods and Privacy Risk	18

Abbreviations

Communications Act	Communications Act of 1934
CPNI	customer proprietary network information
ECPA	Electronic Communications Privacy Act of 1986
FIPP	Fair Information Practice Principles
FTC	Federal Trade Commission
GPS	Global Positioning Satellite
NHTSA	National Highway Transportation Safety Administration
NTIA	National Telecommunications and Information Administration
PND	portable navigation device
OECD	Organisation for Economic Co-operation and Development
VIN	vehicle identification number

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.



December 6, 2013

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

Dear Mr. Chairman:

The prevalence of in-car communication systems (called “telematics”),¹ as well as portable navigation devices (PND) and smart phones, has brought significant opportunities for consumers to access location-based services in their cars. Consumers increasingly use and benefit from these services not only for directions, but also for other services like real-time traffic information, emergency assistance, or to help find the nearest restaurant or gas station. The market for such location-based services is expected to grow as companies make use of new technologies, such as those that integrate smart phones with vehicles and those that use crowd-sourced positioning, which uses location data gathered from a large number of consumers, to provide real-time traffic information. According to one study, for example, the market for telematics services provided by auto manufacturers in North America is expected to increase from 11.8 million subscribers in 2012 to 31.6 million in 2016.²

As in-car location-based services have become commonplace, privacy groups and policy makers have questioned whether the location data collected and used by various companies in the course of providing such services pose privacy risks. Specifically, they are concerned that location data can be used for purposes other than to provide services to the consumer, such as selling the data to others for marketing. They also have concerns that location data can be used to track where consumers are, which can in turn be used to steal their identity, stalk them, or monitor

¹Telematics systems use telecommunication networks and GPS signals to allow information, such as location data, to be communicated between a car and a service provider.

²Frost & Sullivan, *Key Trends and Forecasts for the North American and Latin American Automotive Navigation and Telematics Services Market* (May 2012).

them without their knowledge. In addition, location data can be used to infer other sensitive information about individuals such as their religious affiliation or political activities. Congress and several federal agencies have considered the implications of the collection of location data on consumer privacy. While legislative proposals aimed at protecting the privacy of location data by mobile devices and navigation systems have been introduced by Members of Congress, none of the proposals have been enacted.³

You asked us to review issues related to the privacy of location data collected by in-car location-based services. This report addresses (1) what selected companies that provide in-car location-based services use location data for, and if the companies share the data and (2) how these companies' policies and reported practices align with industry-recommended privacy practices. This work complements a review that we conducted on the privacy of location data collected by mobile devices. In that review, we found that the companies in our sample did not consistently follow industry-recommended privacy practices and that federal agencies could clarify their expectations for steps companies should take to protect consumers' location data privacy. We recommended that the Federal Trade Commission (FTC) consider issuing guidance on protecting the privacy of location data and that the Department of Commerce's National Telecommunications and Information Administration (NTIA) outline goals, milestones, and performance measures for its ongoing process to develop industry codes of conduct.⁴

To address our objectives, we selected 10 companies that provide services that rely on the real-time transmission of location data from a device in the car to a central location. The 10 selected companies include six auto manufacturers, two PND companies, and two map and

³See Geolocation Privacy and Surveillance Act, H.R. 1312, 113th Cong. (2013); Geolocation Privacy and Surveillance Act, S. 639, 113th Cong. (2013). Additionally, a bill was introduced in the 112th Congress that addressed the privacy of location data. See Location Privacy Protection Act of 2012, S. 1223, 112th Cong. (2011).

⁴GAO, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, [GAO-12-903](#) (Washington, D.C.: Sept. 11, 2012). The report's recommendation to FTC has been implemented. NTIA did not agree with our recommendation.

navigation application (app) developers for mobile devices.⁵ While our findings are not generalizable to all companies that provide in-car location-based services, we selected auto manufacturers and PND companies that are the largest in the United States by market share and app developers that have widely used map and navigation apps on mobile devices. For example, the six auto manufacturers we selected constituted nearly 75 percent of new car sales in the United States in 2012. For each company, we examined documentation of the company's privacy practices in effect in 2013, which could include their privacy policies, terms of service agreements, and written disclosures to consumers, among other things. We further interviewed representatives from each of the companies to discuss its practices, as well as representatives from three third-party partners or contractors used by these companies to provide services, where applicable. While the 10 companies in our review may use a number of third-party companies to provide services, we selected three third-party companies to interview because they specifically provide telematics or traffic-information services. The findings from these third parties are not generalizable to all third parties that provide location-based services, but provided us with insights about third-party use of location data. We reviewed documents and interviewed officials from the FTC, which protects consumers against unfair or deceptive business practices, including privacy issues, and NTIA, which advises the President on telecommunications and information policy issues. We also interviewed privacy advocates and automobile industry associations for their views on privacy practices and potential privacy risks that consumers might experience if companies do not implement the practices. See appendix I for a more detailed description of our scope and methodology.

We conducted this performance audit from February 2013 to December 2013 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.

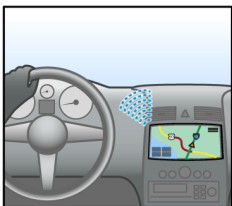
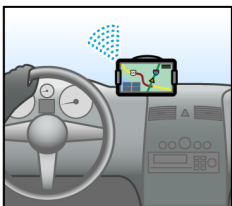
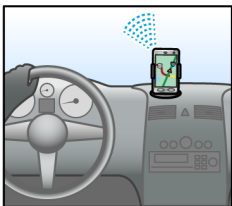
⁵The selected auto manufacturers are Chrysler, Ford, General Motors, Honda, Nissan, and Toyota. The selected PND companies are Garmin and TomTom. The selected map and navigation application developers are Google Maps and Telenav. See appendix I for each of the companies' location-based services that we focused on for this review.

Background

In-Car Location-Based Services

In-car location-based services are delivered by telematics systems, PNDs, and map and navigation apps for mobile devices. See figure 1 for a description and examples of these systems and devices.

Figure 1: Description and Examples of Systems or Devices That Deliver In-Car Location-Based Services to Consumers

Systems or devices that deliver in-car location-based services	Description	Examples
Telematics systems 	<ul style="list-style-type: none"> • Provided by auto manufacturers. • Consumers receive services through devices embedded in their cars or through their mobile devices that are connected to their cars.^a • Services are generally subscription-based, requiring consumers to pay for services. 	General Motors' OnStar, Ford Sync, Chrysler UConnect
Portable navigation devices (PND) 	<ul style="list-style-type: none"> • Provided by PND companies. • Consumers receive services through PNDs that are equipped to transmit location data, or through their mobile devices that are connected to their PNDs.^a • Services can be free to consumers or require a fee for subscription. 	TomTom, Garmin
Map and navigation applications for mobile devices 	<ul style="list-style-type: none"> • Provided by mobile application developers. • Consumers receive services through smart phones. • Services are generally free or relatively inexpensive. 	Scout GPS Navigation, Google maps

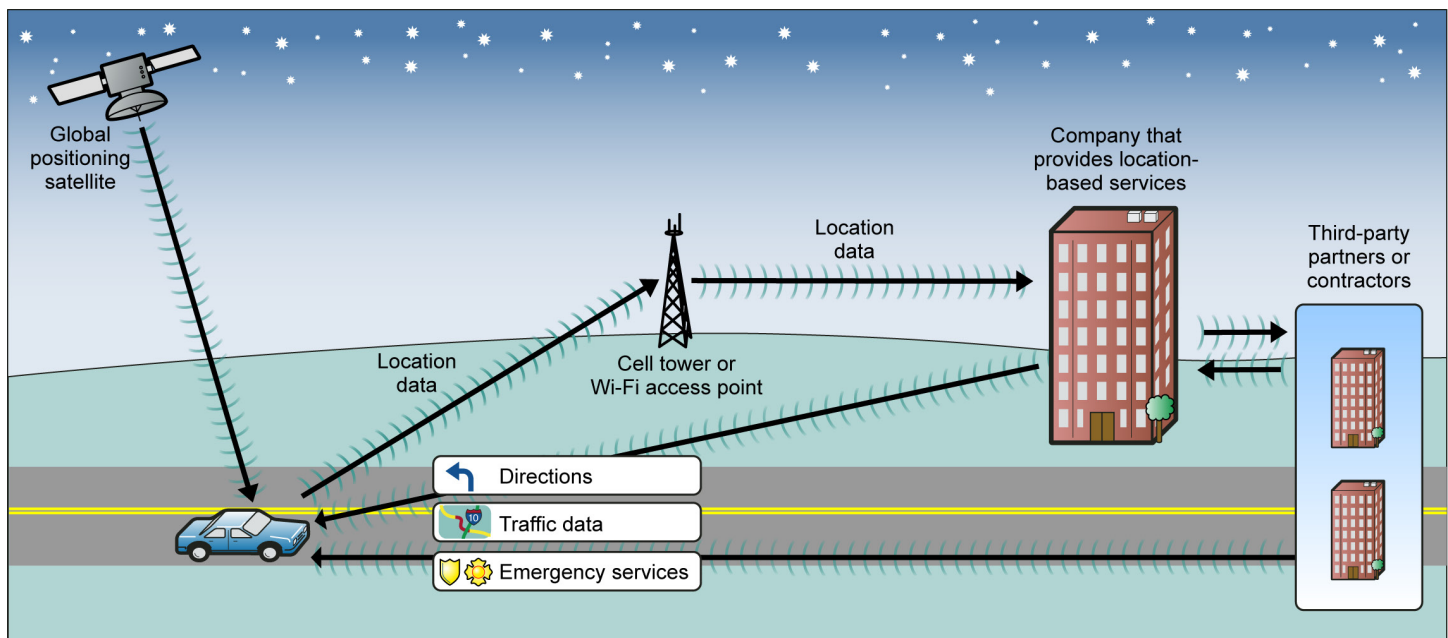
Source: GAO analysis of telematics systems, PNDs, and map and navigation applications that provide in-car location-based services.

^aIn cases where mobile devices are used, consumers use wireless technology to connect their mobile devices to their cars or PNDs. Once connected, consumers can access certain mobile device location-based services on the devices embedded in their cars or on their PNDs.

Telematics systems, PNDs, and map and navigation apps receive Global Positioning Satellite (GPS) signals, which identify the location of consumers in their cars. The consumers' location data, which consist of GPS coordinates, are transmitted over the cellular network or Wi-Fi access points to companies providing the services. Based on the location information received, companies provide requested services to

consumers. Companies may choose to partner with third parties to provide a specific location-based service, such as real-time traffic information. Companies may also choose to contract with third-parties that provide all location-based services on their behalf; among our selected companies, this is most common among the auto manufacturers.⁶ (See fig. 2.)

Figure 2: How Location Data Are Transmitted to Provide In-Car Location-Based Services



Source: GAO.

Note: While companies use cellular networks to transmit location data, we excluded telecommunications companies that provide these networks from this review because they were included in our 2012 report on mobile devices. See [GAO-12-903](#).

The in-car location-based services industry continues to change and evolve: new partnerships are emerging in the marketplace, existing companies are changing how they provide location-based services, and

⁶Some PNDs and navigation systems in cars are not equipped to transmit location data in real time to companies. These devices and systems are able to provide navigation assistance based on satellite or other signals received. However, these types of devices and systems are not within the scope of our review because they pose less privacy risks to consumers as compared to devices and systems that transmit location data to companies.

technologies are advancing. For example, in 2012, a telecommunications company—Sprint—announced that it would partner with Chrysler to provide location-based and other in-car communication services using wireless technology embedded in cars. To expand its presence in the telematics and connected-service market, SiriusXM Radio Inc., a satellite radio broadcasting company, announced in 2013 that it entered into an agreement to acquire Agero Connected Services Inc., a company that auto manufacturers contract with to provide location-based services. In addition, some market analysts state that the market for stand-alone PNDs is waning, and as a result, existing PND companies have established partnerships with auto manufacturers to provide navigation services embedded in cars and have developed apps for mobile devices. Furthermore, as technologies that provide location-based services advance, auto manufacturers look to improve driver experiences by making cars more connected to mobile devices.

Industry Privacy Practices Mobile industry associations and privacy advocacy organizations have recommended practices that companies can take to better protect consumers’ privacy; we determined that these recommended practices can be applied to the companies discussed in this report.⁷ Specific examples of recommended practices are shown in table 1.

Table 1: Industry-Developed Recommended Privacy Practices Applicable to Location Data	
Category	Examples of specific practices
Disclosures to consumers about data collection, use, and sharing	<ul style="list-style-type: none">• State reasons companies collect and share data.• State specifically that collection of location data is limited to specific needs.• Do not use data for a purpose other than what has been disclosed to consumers without providing notice and obtaining consent before using the data.
Controls over location data	<ul style="list-style-type: none">• Obtain consumers’ consent before collecting their personal information.• Provide consumers the ability to opt out of data collection to which they have previously consented.• Allow consumers to delete location data that have been collected.

⁷We identified the recommended practices for our 2012 review on mobile device location data. See [GAO-12-903](#) for examples of the recommended practices. Appendix I of this report contains more information about how we determined that the recommended practices could be applied to companies discussed in this report.

Category	Examples of specific practices
Data safeguards and retention	<ul style="list-style-type: none"> State a specific time frame for retaining consumer data. Protect data with reasonable security safeguards against risks such as loss or unauthorized access.
Accountability	<ul style="list-style-type: none"> Ensure employees protect consumers' data. Keep third parties responsible for protecting consumers' data.

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

Existing and Proposed Privacy Protections

Currently, no comprehensive federal privacy law governs the collection, use, and sale of personal information by private-sector companies; rather, the privacy of consumers' data is addressed in various federal laws. Some of these federal laws are relevant to location data (see table 2).⁸ The privacy of consumers' location and other data is also protected in accordance with companies' privacy practices. Federal law does not require companies to notify consumers of their privacy practices, but companies within the scope of our review have conveyed these practices through privacy policies and other documents. Additionally, FTC has reported that because protecting privacy is important to consumers, companies that deal with consumer data, including location data, have placed emphasis and resources on maintaining reasonable security.

Table 2: Select Laws That Address Consumer Privacy and Their Relevance to Privacy of Location Data

Law	Description	Relevance to the privacy of location data
Federal Trade Commission (FTC) Act	This Act prohibits unfair or deceptive acts or practices in or affecting commerce and authorizes FTC enforcement action. This authority allows FTC to take remedial action against a company that engages in a practice that FTC has found is unfair or deceives its customers.	FTC could take action against a company if FTC found the company was being unfair or deceptive by not adhering to the company's own privacy policies that describe how location data are collected, used and shared.

⁸We reviewed select federal laws that are relevant to companies that provide in-car location-based services. We previously reported on a number of other federal privacy laws which were not relevant to our review. See GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

Law	Description	Relevance to the privacy of location data
The Communications Act of 1934 (Communications Act)	This Act, as amended, imposes a duty on telecommunications carriers to secure information and imposes particular requirements for protecting information identified as customer proprietary network information (CPNI), including the location of customers when they make calls. The Act also requires express authorization for access to or sharing of call location information concerning the user of commercial mobile services, subject to certain exceptions.	The Act covers location data collected by telecommunications carriers, not location data collected by companies that provide in-car location-based services.
Electronic Communications Privacy Act of 1986 (ECPA)	This Act prohibits the federal government and providers of electronic communications from accessing and sharing the content of consumers' electronic communications, unless approved by a court or by consumer consent. The Act also prohibits providers of electronic communications from voluntarily disclosing customer records to government entities, with certain exceptions, but companies may disclose such records to a person other than a governmental entity.	The Act does not specifically address whether location data are considered content or part of consumers' records. Some privacy groups have stated that ECPA should specifically address the protection of location data.

Source: GAO summary and analysis of select laws.

Some privacy groups, some Members of Congress, and others maintain that privacy rights are being compromised by new uses of technology that are not addressed in existing laws. In 2012, FTC and NTIA called on Congress to pass data privacy legislation that would provide a minimum level of protection for consumer data, including location data. Some Members of Congress have introduced bills that would address the privacy of consumers' electronic personal data, including location data. In particular, three of these bills would generally require commercial entities—such as those companies within the scope of this report—to provide notice and obtain consent from consumers to collect and share their location data.⁹

NTIA and FTC have both issued reports that offered recommendations aimed at improving overall consumer privacy, including location-based services. In February 2012, NTIA prepared a report for the White House that offered a framework and expectations for companies that use consumers' personal information, which includes location information.¹⁰

⁹See H.R. 1312, 113th Cong. (2013); S. 639, 113th Cong. (2013). Additionally, a bill was introduced in the 112th Congress that addressed the privacy of location data. See S. 1223, 112th Cong. (2011).

¹⁰The 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).

The framework includes a consumer privacy bill of rights that states that consumers are entitled to, among other things, exercise control over what personal information companies collect and how they use it, and to easily understand and access information about companies' data privacy and security practices. In March 2012, FTC issued a report that described recommended practices for companies that collect and use consumer data.¹¹ This report recommended, for example, that companies obtain affirmative express consent from consumers before collecting precise location data; limit collection to data needed for a requested service or transaction; and provide consumers with prominent notice about the sharing of their location data. Companies' use of NTIA's and FTC's practices for protecting consumers' data is voluntary. Like the industry-developed recommended location data privacy practices described in table 1, the recommendations offered by NTIA and FTC are consistent with the internationally recognized privacy practices called the Fair Information Practice Principles (FIPP).¹²

Selected Companies Stated That They Primarily Collect and Share Location Data to Provide and Improve Consumer Services

Representatives from all of the selected companies told us that they collect location data primarily to provide consumers with various requested location-based services. Telematics systems provided by the auto manufacturers we reviewed collect location data to respond to specific requests from consumers for location-based services such as turn-by-turn directions, information on local fuel prices, stolen vehicle tracking, or roadside assistance. Additionally, representatives from three auto manufacturers told us that their electric vehicle telematics systems use location data to help drivers of electric vehicles locate nearby charging stations. Separately, representatives from five auto manufacturers told us that their telematics systems also collect location data for other purposes. For example, a representative from one auto manufacturer told us that when a vehicle's diagnostic trouble code is displayed (e.g., the check engine indicator light is displayed) or during monthly checks by the telematics system, the company collects location

¹¹Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, D.C.: March 2012).

¹²We used the industry-developed privacy practices—not the NTIA and FTC recommended practices—to evaluate our 10 selected companies' reported privacy practices because the industry-developed privacy practices are specific to location data. NTIA's and FTC's recommended practices address consumer data, which include but are not specific to location data.

data along with vehicle data to determine whether driving in certain locations, such as near power plants, affects a vehicle's overall performance. The companies we reviewed that sell PNDs and navigation apps for mobile devices similarly collect location data to provide consumers with requested traffic and navigation services. Some of these companies may also collect location data to provide consumers additional features such as the location of nearby restaurants or points of interest.

Representatives from all 10 selected companies told us that they share consumer location data with third parties to provide and improve services, with law enforcement, or with others for other purposes when data are de-identified.¹³

- Sharing to provide and improve services: Representatives from nine of the selected companies told us that they share location data to provide location-based services to consumers or to improve the accuracy of services provided to consumers; representatives from the remaining company said that it does not share location data of consumers using its traffic and navigation services because it provides these services in-house. The six selected auto manufacturers generally share location data with third parties that provide consumers with location-based services. For example, of these auto manufacturers, three authorize the same third-party contractor to collect and use vehicle-specific location data to provide telematics services on the auto manufacturers' behalf. Although the level of services varies by manufacturer, this third-party company provides services to consumers such as navigation assistance, traffic assistance, and concierge services where consumers can obtain assistance from live operators for business and personal needs such

¹³"De-identified" location data are those data that have had personally identifiable information, such as a consumer's name or home address, removed or masked. When data are de-identified, a consumer's personally identifiable information could be reconstituted in certain circumstances (that is, the consumer can be re-identified). If location data are de-identified in a way that a consumer cannot be re-identified, then the data are anonymous. Aggregating de-identified data, which combines de-identified data from a number of individuals or vehicles, are anonymous because the data cannot be linked to an individual at all. Aggregated vehicle location data could be used, for example, to determine the speed of vehicles at 5 p.m. on a certain section of a road. The de-identification methods companies use may or may not result in location data that are anonymous. For more information on de-identified, anonymous, and aggregated data, see National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication 800-122 (Gaithersburg, Maryland: April 2010).

as making flight or restaurant reservations. Auto manufacturers' telematics systems may also share vehicle-specific location data with public-safety emergency-service providers and third-party roadside assistance providers so that they can provide emergency and breakdown assistance. Representatives from both PND companies and one app developer said that they share aggregated location data associated with traffic flows with third parties, including traffic information providers. Traffic information providers use such data, along with data from various other sources (such as traffic alerts and GPS data collected from vehicle fleets) to augment and improve the accuracy of real-time traffic services provided to consumers.

- Sharing with law enforcement: All 10 of the selected companies' disclosures describe circumstances under which they may share location data with law enforcement. For example, one company's disclosure states that the company can, when required, share location data "to comply with the law, in legal proceedings, to respond to subpoenas or court orders, and in cooperation with law enforcement agencies." Another company's disclosure states that it is not required to release any records that are created as part of its service without a subpoena (unless otherwise required by law). However, for companies that do not retain personally identifiable location data, there are no data for law enforcement to use.
- Sharing for other purposes: Representatives from two of the selected companies told us that they share location data for other purposes beyond providing services to consumers. Representatives from these two companies told us that they have provided location data that they have de-identified or aggregated to university research programs, the National Highway Transportation Safety Administration (NHTSA), and state departments of transportation for research purposes (e.g., causes of accidents) and to improve information about traffic patterns for infrastructure planning.¹⁴ Representatives from both companies told us that they have contractual agreements in place with these entities that govern how the data should be used and protected. Separately, representatives from all of the selected companies told us that they do not share identifiable location data with or sell such data to marketing companies or data brokers that collect information for the purposes of reselling the information to others. However,

¹⁴Specifically, representatives from one company told us that it shares location data that are associated with unique vehicle identifiers or location data that are aggregated. The other company shares location data that have been de-identified and aggregated.

representatives from one of these companies told us that it shares aggregated data with marketing companies.

As discussed in more detail below, while the companies we reviewed stated that they did not share data for purposes other than those mentioned, their policies give them the flexibility to do so. In addition, some companies do not describe the purposes for sharing de-identified location data in their disclosures to consumers. Furthermore, as we discuss later in this report, companies use various methods to de-identify location data, some of which could result in a consumer being re-identified (that is, their personally identifiable information could be reconstituted).

Selected Companies Have Implemented Some Recommended Practices, but the Extent to Which Consumers' Privacy Could Be at Risk May Not Be Clear

Industry-recommended practices state that companies should protect the privacy of location data by providing (1) disclosures to consumers about data collection, use, and sharing; (2) controls over location data; (3) data safeguards and explanations of retention practices; and (4) accountability for protecting consumers' data. The recommended practices are not required, but rather provide a framework for understanding the extent to which these companies protect the privacy of consumers' location data. We found that all 10 companies have taken steps that are consistent with some, but not all, of the recommended practices, and the extent to which consumers' data could be at risk may not be clear to consumers.

Selected Companies Disclose That They Collect and Share Location Data, but Disclosures to Consumers Are Sometimes Unclear

Recommended practices state that companies should clearly disclose how they collect, use, and share location data and the purposes for doing so. We found that companies use various methods to disclose their privacy practices, but the information about the use and sharing of location data was sometimes unclear. Without clear disclosures about the collection and sharing of location data, consumers may not be aware of all the purposes for which their data are collected and shared. Thus, data may be used and shared for purposes that the consumer is not expecting or to which the consumer might not have chosen to agree. Privacy advocates as well as the FTC and NTIA have stated that privacy disclosures should be clearly written, readily available, and describe all purposes for which personal data are collected and shared.

Notification Methods

All 10 selected companies use privacy policies, terms of service agreements, and other practices—such as on-screen notifications—to notify consumers of their privacy practices. Of the 10 companies we

reviewed, six have stand-alone privacy policies and four use terms of service agreements that include an explanation of their privacy practices. Of the six companies that have stand-alone privacy policies, four companies and one of the auto manufacturers for its electric vehicle provide notice via an on-screen display. According to one auto manufacturer, its services are requested and provided through voice command and audible response rather than through a screen, making on-screen notifications impractical with current systems. Further, the nature of the service makes it difficult and inconvenient to notify consumers about location data collection each time service is requested. For example, the auto manufacturer said that it would not be practical for notification to occur in connection with the delivery of emergency services since those tend to be provided automatically, without consumer request, when there is an accident.

Purposes for Collection and Use

All 10 selected companies disclose the reasons for collecting location data, which are generally based on the types of services they provide. However, 9 of 10 companies also provide reasons for collecting location data that are broadly worded and potentially allow for unlimited data collection and use. For example, one company's terms of service states that the provided reasons for location data collection were not exhaustive. Furthermore, none of the selected companies explicitly state in their disclosures that location data are not collected for other purposes. Three of the selected companies state in their disclosures that they seek consumers' consent before using location data for purposes beyond those listed. Without clear disclosures about the purposes, consumers may not be able to effectively judge whether the uses of their location data might violate their privacy. Furthermore, risks increase that data may be used for purposes the consumer is not expecting or to which the consumer might not have chosen to agree.

Purposes for Sharing Location Data

All 10 selected companies disclose that they share consumer location data with third parties, mainly to provide requested services. Six companies' disclosures allow for additional sharing for location data when they are de-identified, but the purposes for sharing such data were not described in five of these companies' disclosures. Although not disclosed, representatives from three of the five companies explained to us that they share de-identified or aggregated location data for providing services or for other purposes. Representatives from the remaining two companies said that although their disclosures give them the option to share de-identified location data, their companies do not share such location data at all. Because companies have not made clear disclosures about the purposes for sharing de-identified location data, risks increase that data

may be used for purposes that the consumer is not expecting or to which a consumer might not have chosen to agree.

Selected Companies Obtain Consent and Provide Certain Controls for Collecting Location Data, but Consumers Are Not Able to Delete Their Collected Data

Recommended practices state that companies should obtain consumers' consent for collecting, using, and sharing personal information, including location data, and allow consumers to control their data, such as by opting-in and opting-out of collection and deleting location data. We found that companies obtain consumer consent and provide controls in a variety of ways, but do not allow consumers to request their historical location data to be deleted when data are associated with an individual or vehicle. Without the ability to delete their location data, consumers are unable to prevent the use or retention of their data, should they wish to do so. Privacy advocates, as well as the NTIA and FTC, have stated that consumers should provide their consent and have an appropriate level of control over how their personal data are collected, used, and shared. NTIA and privacy advocates have also stated that consumers should be able to request deletion of data collected about them.

Consent

The selected companies obtain consumer consent to collect location data in various ways, but some methods are more explicit than others. For example, auto manufacturers obtain consumer consent when consumers agree to the terms of service either when purchasing the vehicle equipped with the service or when signing-up and paying for the service. According to one privacy group we met with, if consent is obtained when a consumer purchases a vehicle, consumers may not be as likely to review a company's stated privacy practices because they may be a part of a larger set of documentation about the vehicle and its telematics system. Both PND companies and one auto manufacturer (for its electric vehicle) obtain consumer consent to collect location data more explicitly, via an on-screen prompt that allows consumers to accept or decline the transmission of such data. Both of the selected app developers we reviewed obtain consumer consent when consumers agree to the terms of the privacy policy or the terms of service (which includes a developer's privacy policy) when initially downloading the app.

Controls

The selected companies provide consumers various ways to opt in or out of location data collection. For example, auto manufacturers provide consumers with controls over location data collection by offering the telematics system as an option on a new vehicle purchase. However, auto manufacturers are including these systems as standard equipment on vehicles. In fact, one auto manufacturer told us it now provides a limited-time free subscription to its telematics service on most of its new cars, but that consumers can cancel at any time. According to the

company, once a consumer cancels the subscription, location data are not collected, despite the equipment still being in the vehicle. Additionally, auto manufacturers told us that consumers can further choose to use these services or not. That is, a consumer has the option to request the location-based service and have location data transmitted, can refrain from using the service, or can cancel the service entirely.

Both selected PND companies allow consumers to decide if they want their location data transmitted. For one PND company, consumers can opt in to the collection and sharing of location data for traffic information purposes via an on-screen prompt. Consumers who do not opt in will not receive traffic data but they can still use other location-based services, such as weather, if they choose to do so. For the other PND company, consumers can control the collection of all location data via an on-screen prompt or by adjusting the device's settings. If location data are turned off, consumers can still use the device for basic navigation but can no longer receive real-time traffic information. For the mobile device apps, consumers opt in to transmitting location data by downloading the app and requesting location-based services, and have the ability to opt out by not requesting services, changing the device's setting to prevent location data from being transmitted, or deleting the app entirely. When consumers download one particular app, the app asks whether it can collect anonymous location data at any time, including when not providing a specific navigation service. In this case, the default is to collect the anonymous location data unless the consumer takes an additional step to opt out. The app developer seeks to collect such data to improve its traffic-information and other services. The consumer can also adjust the device's settings at any time to prohibit the app from collecting the anonymous location data.

Deletion of Data

None of the 10 selected companies allow consumers to delete the location data that are, or have been, collected. Some companies de-identify and aggregate location data or do not retain any location data so it would not be possible for consumers to delete or request that their data be deleted. However, representatives from four companies told us that they keep the location data in a format that is associated with an individual vehicle yet do not allow consumers to delete their data or request their deletion. In such cases, consumers are unable to prevent the retention or use of retained data, should they wish to do so.

Selected Companies Stated That They De-Identify Location Data, but Different Methods and Retention Practices May Lead to Varying Levels of Protection for Consumers

Recommended practices state that companies should safeguard location data, in part, by de-identifying them; that companies should not keep location data longer than needed; and that such data should be deleted after a specific amount of time. We found that while selected companies safeguard location data in part by de-identifying them, companies use different de-identification methods that may lead to varying levels of protection for consumers. We also found wide variation in how long companies retain vehicle-specific or personally identifiable location data. Privacy groups we interviewed raised concerns about retaining location data for long periods of time because there are more opportunities to use the data to identify individuals or their behaviors and because longer retention periods put data at increased risk for unauthorized access or accidental disclosure. In addition, privacy groups said that de-identifying location data may not always protect consumers against privacy risks because some methods of de-identification can allow for an individual to be re-identified.

Safeguarding Location Data: De-Identification and Encryption

All of the selected companies stated in their disclosures, or in interviews with us, that they use or share de-identified location data. Representatives from some of the selected companies explained how they de-identify location data; the methods differed among the companies that responded, for example:

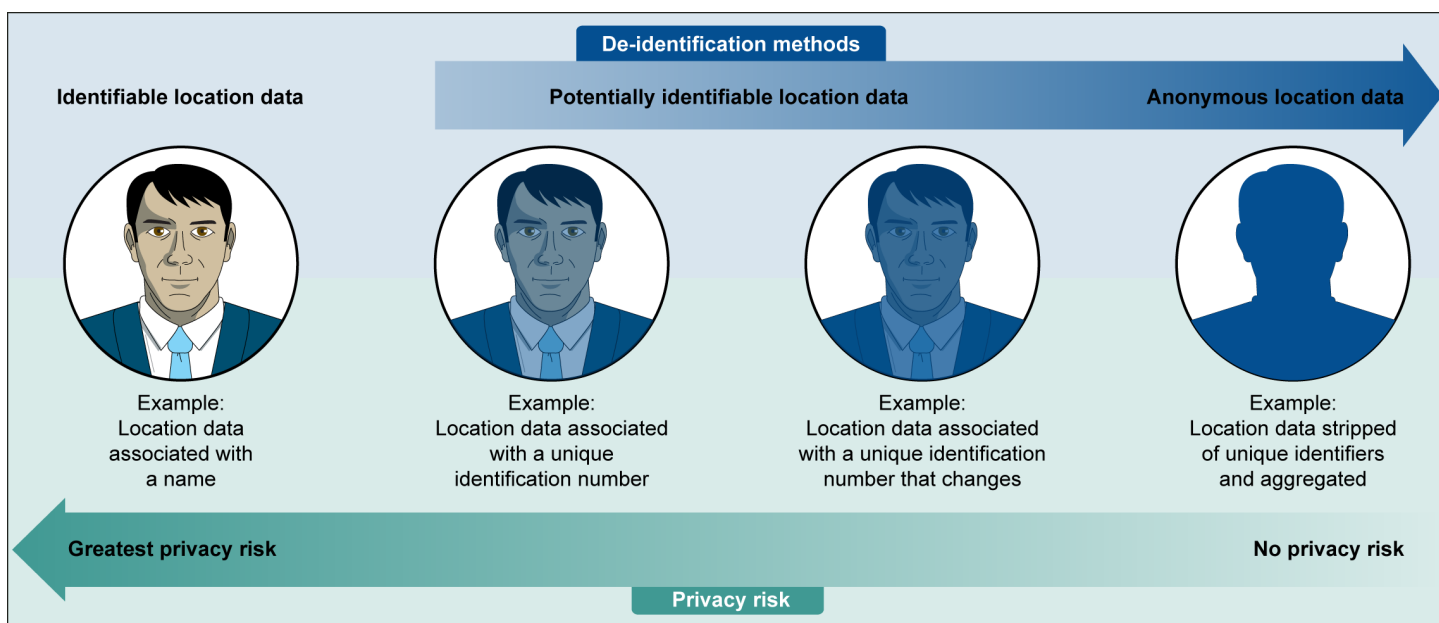
- A representative from one app developer told us that for its map and navigation application, the company does not associate location data with consumers, unless the consumers have signed into their accounts. In addition, this company uses other methods to further reduce the likelihood that individuals (who have not signed into their accounts) will be identified, such as collecting location data periodically rather than continuously.
- Representatives from four companies told us that they de-identify location data by removing consumers' names from the location data, and associating the data with unique identification numbers. Three of these companies authorize their third-party contractor to collect location data along with a unique vehicle identification number or VIN that all vehicles possess. This third party associates the VIN with other information to determine which vehicle to provide location-based services to. Representatives from the fourth company told us that before they share data for research purposes, they associate location data with unique vehicle identifiers or aggregate them.
- Representatives from three companies told us that they de-identify location data they receive from consumers (after consumers provide their consent) by associating the location data with randomly

generated identification numbers that change after a specific period of time.

- Representatives from three companies told us that before they share any location data with third parties, they strip the data of any identifiers and aggregate the data so that they are not tied to and not able to be tied to any particular consumer.

The de-identification method a company uses affects the extent to which consumers may be re-identified and exposed to privacy risks. Location data that are collected along with a consumer's name or other identifying information are, by definition, personally identifiable data and present the greatest privacy risks to consumers because a consumer's identity is known. Privacy risks decrease when companies de-identify location data, but the level of risk falls on a spectrum depending on how easy it is to re-identify consumers. De-identifying location data with unique identification numbers prevents the direct association of location data with a specific vehicle or individual. However, if the same identification number is re-used for the same consumer on multiple trips, then the consumer's history or patterns can potentially be discerned. In such instances, consumers face an increased likelihood that they can be re-identified. Privacy risks decrease if location data are associated with identification numbers that change over time because it is more difficult to discern an individual's history and identify an individual. Finally, consumers face little to no privacy risks when location data are stripped of any identification numbers and aggregated with other consumers' data because the data are anonymous, meaning that the data cannot be linked to an individual at all. (See fig. 3.) To the extent that companies use personally identifiable location data or use de-identification methods that allow a consumer to be re-identified, risks increase that consumer location data may be used in ways the consumer did not intend, such as to track their travel patterns or to target consumers for unwanted marketing solicitations.

Figure 3: Examples of De-Identification Methods and Privacy Risk



Source: GAO.

Although location data that are coupled with personal information, such as a name, pose the greatest privacy risk to consumers, company representatives told us that in some cases, they need such data to provide certain services. For example, one auto manufacturer we met with said that one of its services—concierge services—is personalized to the consumer requesting the service and therefore relies on data that are associated with the individual requesting the services. Representatives from one third-party contractor that works with auto manufacturers said that consumers can receive a broader array of services by voluntarily providing additional data to service providers in connection with enrollment in the services. In contrast, representatives from PND companies and app developers told us that they do not need to know personally-identifiable information about a consumer to provide traffic and navigation services, just their location. As such, they said that their companies collect de-identified location data.

In addition to de-identifying location data, all of the selected companies stated in their disclosures, or in interviews with us, that they safeguard location data or personal data that may include location data. Eight companies' disclosures state that they implement physical, technical, or other safeguards and the remaining two told us they have these

safeguards but did not state that they have them in any of their disclosures. Companies can safeguard location data by encrypting¹⁵ them while they are being transmitted between a vehicle or device and the company that provides location-based services. In our analysis of data transmitted from two selected mobile apps to the developers who provide location-based services, we found that one developer encrypted all data transmitted from the app, so we could not discern what was being transmitted. The other developer did not encrypt the data transmission, and we were able to view the location data and other data, such as usernames and passwords, being transmitted. This developer acknowledged that such data were not encrypted and told us that it had made a decision independent from our review to encrypt the data in future releases of the app. To the extent that data are not encrypted, consumers may be at risk that their data may be subject to unauthorized access, disclosure, and modification.

Retaining Location Data

None of the selected companies' disclosures discuss how long data are retained, but some company representatives we interviewed told us that that they do not retain location data "longer than necessary." A contractor that works with three companies in our review to provide location-based services told us that when a consumer requests services, in accordance with the contractual terms in place with the companies, the contractor may retain vehicle-specific location data, VIN, and other data associated with the consumer's request for up to 7 years. The contractor explained that it retains such subscriber information to protect against potential lawsuits, to allow the companies to evaluate how the contractor is performing, and for tax purposes should a tax authority audit their income associated with the provision of services. Representatives from one company stated that it retains personally identifiable location data for no more than 24 hours, and a representative from another company said that it does not retain such data at all. However, representatives from both of these companies told us that they retain de-identified location data indefinitely.¹⁶ As we concluded in our 2012 report,¹⁷ the longer identifiable

¹⁵Encryption protects data through a process of transforming ordinary data (commonly referred to as plaintext) into code form (ciphertext) so that the data are unintelligible to users without the proper decryption key.

¹⁶Representatives from one of the companies told us that the data it retains are aggregated location data, and representatives from the other company told us that the data it retains are location data associated with unique identification numbers that change.

¹⁷[GAO-12-903](#).

location data are retained, the more vulnerable the data are to use by bad actors, such as hackers, or to unauthorized third-party access. Furthermore, risks increase that the amassed data could be used to create a detailed profile of individual behavior.

Selected Companies Have Taken Steps to Be Accountable for Protecting Location Data, but the Steps They Take within Their Companies Are Generally Not Disclosed to Consumers

Recommended practices state that companies should demonstrate accountability for their practices as well as the practices for third parties they use to provide services. If accountability practices are disclosed to consumers, then consumers may have greater assurance that their location data are reasonably protected. We found that most of the selected companies disclose to consumers that they hold third parties accountable for safeguarding data that are shared. However, none of the companies disclose to consumers how they hold themselves and their employees accountable to their privacy policies, although company representatives told us they are taking steps to ensure that they and their employees are protecting consumers' data and following their own privacy policies. Privacy groups and NTIA officials have stated that it is important for consumers to be assured that their location data are appropriately used and protected. To the extent that companies do not disclose the ways in which they hold themselves or third parties accountable, consumers will not be aware of how companies ensure that their data are appropriately protected.

Accountability with Third-Party Service Providers

All companies that share location data with third parties stated in their disclosures, or in interviews with us, that they take steps to protect location data that they share with third parties. For example, seven selected companies' disclosures or company representatives stated that third parties are contractually required to follow the companies' privacy policy or follow certain privacy practices. One of these companies has a business agreement with a third-party contractor that prohibits the contractor from collecting, using, and commingling data, including location data, about consumers or their behaviors for marketing purposes. In addition to holding third parties accountable through contracts, another company told us that in certain circumstances, it requires its third parties to conduct assessments to ensure that they are effectively protecting location data. Rather than conduct an assessment, some third parties choose to obtain certifications from professional security organizations. Separately, representatives from three companies told us that they protect location data that they share with third parties by de-identifying and aggregating them before they are shared.

Accountability within a Company

None of the companies stated in their disclosures how they hold themselves and their employees accountable for adhering to their privacy policies; however, company representatives we interviewed explained various ways in which they ensure that they and their employees are protecting consumers' data. Representatives from all of our selected companies told us that their employees must follow the companies' internal policies to protect data, including location data, and some of the representatives further explained that employees who violate such policies are subject to disciplinary action and possibly termination. Separately, representatives from one of the selected companies told us that it had conducted an independent audit of its practices to provide reasonable assurance that it was in line with company privacy policies. For example, to assess whether the company followed its policy to encrypt location data and make them anonymous, the independent auditor assessed whether the company encrypted location data in a way that only the company could decrypt and that location data were anonymous so that individuals could not be identified and tracked.¹⁸ While companies are taking actions to ensure that they are protecting consumers' data, consumers may be unaware of these actions if they are not disclosed.

Our work provides information to policymakers on the various privacy risks consumers may face when companies collect and share location data to provide in-car location-based services. This information could be important to policymakers as they gauge whether privacy risks are appropriately balanced against the benefits that these services provide. Given that the report focuses on companies' privacy practices, we are not making recommendations to federal agencies at this time.

Agency Comments

We provided drafts of this product to the Department of Commerce and FTC for comment. We also provided relevant portions of the draft to the 10 selected companies and three third-party companies for comment. We received technical clarifications from both federal agencies, all 10 of the selected companies, and two of the three selected third-party companies. We incorporated these technical clarifications as appropriate.

¹⁸The audit determined that the company effectively encrypted and de-identified the location data.

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 Secretary of Commerce and the Chairman of the FTC. 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 me at (202) 512-2834 or rectanusl@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 II.

Sincerely yours,

A handwritten signature in black ink that reads "Lori Rectanus". The signature is written in a cursive, flowing style.

Lori Rectanus
Acting Director, Physical Infrastructure

Appendix I: Objectives, Scope, and Methodology

Our objectives were to examine (1) what selected companies that provide in-car location-based services use location data for and if they share it and (2) how these companies’ policies and reported practices align with industry-recommended privacy practices. This work complements a review that we conducted on the privacy of location data collected by mobile devices.¹

To address these objectives, we examined the privacy practices of companies that provide in-car location-based services. We focused on 10 companies that provide services that rely on the real-time transmission of location data from a car to a central location. These companies fall into three broad categories: (1) auto manufacturers, (2) portable navigation device (PND) companies,² and (3) map and navigation application (app) developers for mobile devices. We selected auto manufacturers and PND companies that are the largest in the United States by market share and app developers that have widely used map and navigation apps on mobile devices. See table 3. While our findings are not generalizable to all companies that provide in-car location-based services, the selected companies we reviewed are those that provide the most widely used services or represent a vast majority of the market. For example, the six auto manufacturers we selected represent nearly 75 percent of new car sales in the United States, and are therefore likely to have telematics systems that are more widely purchased by consumers.

Table 3: Selected Companies That Provide In-Car Location-Based Services		
Category	Company	Location-based service
Auto manufacturers	Chrysler	UConnect
	Ford	Sync
	General Motors	OnStar
	Honda	AcuraLink
	Nissan	Infiniti Connection, CARWINGS
	Toyota	Lexus Enform with Safety Connect, Toyota Entune

¹[GAO-12-903](#).

²Some PNDs only receive GPS satellite signals and are not equipped to transmit location data to companies. These types of devices are not within the scope of our study because they do not transmit location data in real-time.

Category	Company	Location-based service
PND companies	Garmin	Traffic
	TomTom	LIVE Services
Map and navigation application developers ^a	Google Maps	Navigation function
	Telenav	ScoutGPS Navigation

Source: GAO.

^aWe also reviewed the policies and practices of Waze since it was one of the most popular apps, but during our review Waze was acquired by Google and was in the process of revising its policies and so declined to be interviewed for this report.

We identified privacy practices for the 10 companies within the scope of our review by interviewing representatives from these companies and reviewing their privacy policies and other documentation that described their privacy practices in effect in 2013, such as terms of service agreements with consumers and agreements with third parties about how data should be used. We also interviewed representatives of and reviewed documents from third-party service providers that some of these companies use. In particular we interviewed representatives and reviewed documents from Agero Connected Services, Inc; Inrix; and HERE (a Nokia company). While the 10 companies in our review may use a number of third-party companies to provide services, we selected three third-party companies to interview because they specifically provide telematics or traffic-information services. The findings from these third parties are not generalizable to all third parties that provide location-based services, but provided us with insights about third-party use of location data.

To evaluate the 10 companies' privacy practices, we compared them to practices recommended by privacy advocates and groups representing the mobile industry. We identified the recommended practices in our 2012 report on mobile-device location data.³ We determined that the recommended practices were applicable to companies providing in-car location-based services based on interviews with privacy advocacy groups and because our 2012 mobile device report found that the recommended practices generally aligned with the internationally recognized privacy practices called the Fair Information Practice

³[GAO-12-903](#).

Principles (FIPP).⁴ To conduct the evaluation, two analysts conducted separate analyses of the 10 companies' privacy policies, other documentation on companies' privacy efforts, and information gained from our interviews to determine how the companies' practices compared to the recommended practices. Then, the two analysts obtained consensus on those determinations where there had not been agreement. In general, our evaluation examined the companies' privacy practices as stated in their privacy policies, other documentation, or in their interviews with us. We did not independently determine the extent to which companies implemented reported privacy practices, but we corroborated them with our own observations of these services and information from third parties where possible. For example, we were able to observe the actual practices that two selected mobile applications used to protect data transmitted from the applications to the developers. Specifically, we used a computer program to log, monitor, and document all network activity between the two mobile applications and the developers' servers.

To better understand companies' implementation of privacy practices and potential privacy risks⁵ that consumers might experience if companies do not implement the practices, we met with a number of groups or individuals who are knowledgeable about the privacy of location data. Specifically, we met with privacy advocates (Future of Privacy Forum, Electronic Privacy Information Center, American Civil Liberties Union, Electronic Frontier Foundation, Center for Democracy and Technology); a company that certifies businesses privacy programs (TRUSTe); and one privacy researcher (Dorothy Glancy). We also met with associations knowledgeable about the automotive industry or in-car location-based technologies (Alliance of Automobile Manufacturers, Global Automakers, Center for Automotive Research, and the Intelligent Transportation Society of America) to better understand the direction of the automotive

⁴The FIPPs 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. FIPPs are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other interests. The Organisation for Economic Co-operation and Development (OECD), an international organization, developed a revised version of the FIPPs in 1980 that has been widely adopted. See [GAO-12-903](#) for more information.

⁵This review was not designed to identify whether there were any actual violations of consumers' privacy.

industry and technologies. Although the information provided by these groups, individuals, and associations are not generalizable, their views provided us with a perspective on the benefits and risks associated with location data use and sharing. In addition, we reviewed documents and interviewed officials from Federal Trade Commission and the Department of Commerce's National Telecommunications and Information Administration. We also conducted a literature review on techniques to de-identify data.

We conducted this performance audit from February 2013 to December 2013 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: GAO Contact and Staff Acknowledgments

GAO Contact

Lori Rectanus, (202)-512-2834 or rectanusl@gao.gov

Staff Acknowledgments

In addition to the contact named above, Andrew Von Ah (Assistant Director), Thomas Beall, Melissa Bodeau, Mark Canter, Michael Clements, Roshni Davé, Leia Dickerson, John de Ferrari, Andrew Huddleston, Terence Lam, Joshua Ormond, David Plocher, Paul G. Revesz, Nancy Santucci, 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 (<http://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 <http://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: <http://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

