United States Government Accountability Office

Report to the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives

July 2017

VEHICLE DATA PRIVACY

Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role

Accessible Version

GAO-17-656

July 2017

VEHICLE DATA PRIVACY

Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role

GAO Highlights

Highlights of GAO-17-656, a report to the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

The prevalence of connected vehicles—those with technology that wirelessly transmits and receives data—has raised questions about how the collection, use, and sharing of these data affect consumer privacy.

GAO was asked to review consumer privacy issues related to connected vehicles. This report: (1) examines the types, use, and sharing of data collected by connected vehicles; (2) determines the extent to which selected automakers' privacy policies for these data align with leading practices; and (3) evaluates related federal roles and efforts, among other objectives. GAO interviewed relevant industry associations, organizations that work on consumer privacy issues, and a non-generalizable sample of 16 automakers selected based on their U.S. passenger vehicle sales. In addition, GAO analyzed selected automakers' privacy policies (written notices and reported practices) against a set of leading privacy practices determined to be relevant to connected vehicles. To identify these practices, GAO reviewed a variety of privacy frameworks developed by federal agencies and others. GAO reviewed relevant federal statutes, regulations, and reports, and interviewed agency officials, including those from DOT, the Department of Commerce, and FTC.

What GAO Recommends

GAO recommends that NHTSA define, document, and externally communicate its roles and responsibilities related to the privacy of data generated by and collected from vehicles. NHTSA concurred with our recommendation.

View GAO-17-656. For more information, contact Dave Wise at (202) 512-2834 or wised@gao.gov.

What GAO Found

Thirteen of the 16 selected automakers in GAO's review offer connected vehicles, and those 13 reported collecting, using, and sharing data from connected vehicles, such as data on a car's location and its operations (e.g., tire pressure). All 13 automakers described doing so on a relatively limited basis. For example, they reported using data to provide requested services to consumers and for research and development. None of the 13 reported sharing or selling data that could be linked to a consumer for unaffiliated third parties' use. However, as connected vehicles become more commonplace, the extent of data collection, use, and sharing will likely grow.

Automakers have taken steps, including signing onto a set of privacy principles, to address privacy issues. In comparing selected automakers' reported privacy policies to leading privacy practices, GAO found that these automakers' policies at least partially reflected each of the leading privacy practices, for example:

- *Transparency*: All 13 selected automakers' written privacy notices were easily accessible, but none was written clearly.
- *Focused data use*: Most selected automakers reported limiting their data collection, use, and sharing, but their written notices did not clearly identify data sharing and use practices.
- *Individual control*: All 13 selected automakers reported obtaining explicit consumer consent before collecting data, but offered few options besides opting out of all connected vehicle services to consumers who did not want to share their data.

The Federal Trade Commission (FTC) and the Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) are primarily responsible for protecting consumers and ensuring passenger vehicles' safety, respectively. FTC has the authority to protect consumer privacy and has issued reports and guidance and conducted workshops on the topic generally as well as on connected vehicles specifically. NHTSA has broad authority over the safety of passenger vehicles and considers the privacy effects and implications of its regulations and guidance. FTC and NHTSA have coordinated on privacy issues related to connected vehicles. However, NHTSA has not clearly defined its roles and responsibilities as they relate to the privacy of vehicle data. In response to emerging vehicle technologies, NHTSA included privacy requirements in a related rulemaking and included privacy expectations in voluntary guidance. Because of these actions, selected automakers and others said NHTSA's role in data privacy was unclear. NHTSA officials acknowledged that some stakeholders may be uncertain about its authority to address privacy issues. Federal standards for internal control require, among other things, that agencies define and communicate key roles and responsibilities. By clearly defining, documenting, and communicating NHTSA's roles and responsibilities in vehicle data privacy, NHTSA would be better positioned to coordinate with other federal agencies and to effectively oversee emerging vehicle technologies.

Contents

Tables

Figures

Abbreviations

DOT	Department of Transportation
FIPPs	Fair Information Practice Principles
FTC	Federal Trade Commission
NHTSA	National Highway Traffic Safety Administration

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 28, 2017

The Honorable Barbara Comstock
Chairwoman
The Honorable Daniel Lipinski
Ranking Member
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
House of Representatives

Passenger vehicles sold in the United States today are increasingly equipped with technologies that offer consumers a range of safety, security, and convenience services, including roadside assistance and systems that monitor vehicles remotely.[1] As with other everyday objects that are part of the expanding Internet of Things,[2] these "connected vehicles" can wirelessly monitor, collect, and transmit information about their internal and external environment. For example, these vehicles can collect and share data about where drivers go and how they drive, information that used to be impossible or very difficult to collect. As the number of connected vehicles grows, private companies, including automakers, are considering how to use this data to generate revenue. According to a 2016 industry report, the estimated worldwide revenue from connected vehicle data could add up to between $450 billion and $750 billion by 2030.[3] As vehicles generate, collect, and transmit more data, members of Congress,[4] the Federal Trade Commission (FTC), and others have recognized the potential for risks to consumers' privacy. For example, in 2015, FTC staff reported that information collected by connected devices, such as vehicles, pose risks to consumers' privacy

[1]Passenger vehicles include passenger cars, vans, sport-utility vehicles, and pick-up trucks with a gross-vehicle weight rating of 10,000 pounds or less.

[2]See GAO, *Technology Assessment: Internet of Things: Status and Implications of an Increasingly Connected World,* GAO-17-75 (Washington, D.C.: May 15, 2017) and GAO, *Data and Analytics Innovation: Emerging Opportunities and Challenges*, GAO-16-659SP (Washington, D.C.: Sept. 20, 2016). The Internet of Things is generally defined as the concept of connecting and interacting through a network with a broad array of "smart" devices, such as fitness trackers, cameras, door locks, thermostats, and vehicles.

[3]See McKinsey & Company, *Monetizing Car Data: New Service Business Opportunities to Create New Customer Benefits*, September 2016.

[4]Staff of Sen. Edward Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, February 2015.

due to the volume of data collected and the lack of consumers' control over the practice.[5]

You asked us to examine privacy issues related to data collected by and transmitted from vehicles sold domestically. This report examines:

1. the types of data collected by connected vehicles and transmitted to automakers and how, if at all, selected automakers use and share these data;
2. the extent to which selected automakers' privacy policies for connected vehicles align with leading practices;
3. selected experts' views on privacy issues related to the commercial use of data collected by connected vehicles; and
4. federal roles and efforts related to the privacy of data collected by connected vehicles.

This report focuses on privacy issues posed by services offered by automakers to consumers who buy new connected passenger vehicles. We did not focus on privacy issues related to consumers' use of smartphones that link with vehicles through interfaces such as Android Auto and Apple CarPlay or aftermarket devices that collect and transmit data—such as devices offered by insurance providers to track drivers' behavior[6] or that connect older vehicles to services such as roadside assistance or vehicle diagnostics (e.g., Hum by Verizon). We also did not focus on privacy issues related to event data recorders or that may emerge as new connected vehicle technologies—such as automated

[5]FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Washington, D.C.: January 2015).

[6]Such devices enable insurance providers to offer usage-based insurance, in which data on a consumer's driving behavior (e.g., mileage, speed, acceleration, braking, etc.) determine what a consumer pays in premium rates. Data are collected through several methods, including a device installed by the consumer that transmits wirelessly or by integrated connected vehicle technology that is pre-installed in a vehicle.

vehicles, vehicle-to-vehicle technology, or vehicle-to-infrastructure technology[7]—become more common.

To address our objectives, we reviewed applicable federal statutes and regulations, our prior work,[8] and reports by other federal agencies, academics, and research organizations on privacy and connected technologies. We also interviewed representatives of three organizations that advocate protecting the privacy of consumers' data and eight industry associations representing automakers, automotive suppliers, application developers, and telecommunication companies.

To determine the types of data collected from connected vehicles and how, if at all, these data are used, we interviewed representatives of 16 automakers and 3 other industry stakeholders. We selected automakers that sell passenger vehicles in the United States and identified them using the membership lists of two automotive industry trade associations. We identified and selected one additional automaker, which is not a member of these automotive industry trade associations, due to its growing market share and high profile in the connected vehicle market. We identified and selected the other industry stakeholders based on their industry roles (e.g., telecommunication companies, "telematics" service providers,[9] and

[7]Automated vehicle systems are a combination of hardware and software that performs a driving function, with or without a human actively monitoring the driving environment. Vehicle-to-vehicle and vehicle-to-infrastructure technologies—that are connected vehicle technologies—rely on data sent between vehicles, road infrastructure, and personal communication devices to warn drivers and pedestrians of potential accidents. We have previously reported on vehicle-to-vehicle and vehicle-to-infrastructure technologies, see GAO, *Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist*, GAO-14-13 (Washington, D.C.: Nov. 1, 2013) and GAO, *Intelligent Transportation Systems: Vehicle-to-Infrastructure Technologies Expected to Offer Benefits, but Deployment Challenges Exist*, GAO-15-775 (Washington, D.C.: Sept. 15, 2015).

[8]For example, see GAO, *In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers*, GAO-14-81 (Washington, D.C.: Dec. 6, 2013) and GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: Mar. 24, 2016).

[9]The term "telematics" refers to a technology that combines telecommunications and information processing in order to send, receive, and store information related to remote objects, such as vehicles. Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections. They provide a broad range of services, including some supporting safety (such as the ability to report a crash), diagnostics (such as the ability to receive early alerts of mechanical issues), and convenience (such as hands-free access to driving directions or weather).

application developers). After interviewing selected automakers, we summarized and analyzed their responses to identify themes relevant to our research objectives. The views and information gathered through our interviews with selected automakers and industry stakeholders cannot be generalized to the industry as a whole. However, the 16 selected automakers we interviewed produce over 25 vehicle brands and represented around 90 percent of the U.S. passenger vehicle sales market share in 2015.

To determine the extent to which selected automakers' privacy policies for connected vehicles reflect leading practices, we reviewed several widely recognized privacy frameworks developed by the Organisation for Economic Co-operation and Development and several federal agencies, and from these frameworks identified a set of six leading practices that we determined apply to the privacy of data collected by connected vehicles for the purposes of this report.[10] Those leading practices include: transparency, focused data use, data security, data accuracy and access, individual control, and accountability. We obtained information on the reported privacy policies of the selected automakers by reviewing their written privacy notices and interviewing their representatives about their companies' privacy practices. We then compared these privacy policies to the six leading practices.[11] We did not evaluate the extent to which selected automakers followed their reported privacy policies.[12]

[10]Reports used in our leading practice analysis include: (1) Organisation for Economic Co-operation and Development, *The OECD Privacy Framework* (July 11, 2013 revision) *(*known as the *"Fair Information Practice Principles")*; (2) FTC*, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012); (3) FTC Staff Report*, Internet of Things: Privacy and Security in a Connected World* (2015); *(*4) NHTSA, *Federal Automated Vehicles Policy* (2016); and (5) National Institute of Standards and Technology, *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems* (2017). We combined similar practices identified in these frameworks into categories of leading practices.

[11]We interviewed 16 automakers, 13 of which offer connected vehicles. Our analysis of automakers' privacy policies (their written privacy notices and reported privacy practices) included these 13 automakers. However, one of the automakers included in this analysis has different written privacy notices and reported privacy practices for its three affiliated brands. As a result, we analyzed a total of 15 sets of privacy policies (their written notices and reported privacy practices).

[12]This was not a compliance review of automakers and the leading practices we used are not legally binding. As explained later, however, FTC may bring an action against an automaker that violates its own stated privacy policy.

To identify selected experts' views on privacy issues related to connected vehicles, we interviewed 16 subject matter experts.[13] We selected subject matter experts based on eight factors, including their backgrounds in connected vehicles and privacy issues, relevant publications, experience, and presentations. Interviews with selected experts covered a range of issues related to privacy and data collected from connected vehicles. As part of these interviews, we presented these experts with general privacy concerns about the commercial use of data we identified from GAO and other federal agencies' reports and interviews with organizations that advocate protecting the privacy of consumers' data. After interviewing selected experts, we summarized and analyzed their responses to identify themes relevant to our research objectives. The views and information gathered through our interviews with subject matter experts cannot be generalized to all such experts, but they do provide insights into relevant privacy concerns and solutions.

To examine federal roles and efforts related to the privacy of data collected from connected vehicles, we reviewed documents and interviewed officials from four federal agencies—FTC, Department of Transportation (DOT), the Department of Commerce, and the Federal Communications Commission—that we identified as having privacy and consumer protection responsibilities that could relate to connected vehicles. Because of DOT's role in overseeing motor vehicles, we compared DOT's efforts to reevaluate and define key agency roles and responsibilities as new vehicle technologies emerge with pertinent *Standards for Internal Control in the Federal Government*[14] and practices identified in our prior work on agency collaboration.[15] Further details about our scope and methodology are in appendix I.

We conducted this performance audit from April 2016 to July 2017 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

[13]Selected experts include both individuals and organizations with relevant experience. For the full list of selected experts we interviewed, see appendix I.

[14]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). These standards provide the overall framework for establishing and maintaining an effective internal control system for the federal government.

[15]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

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.

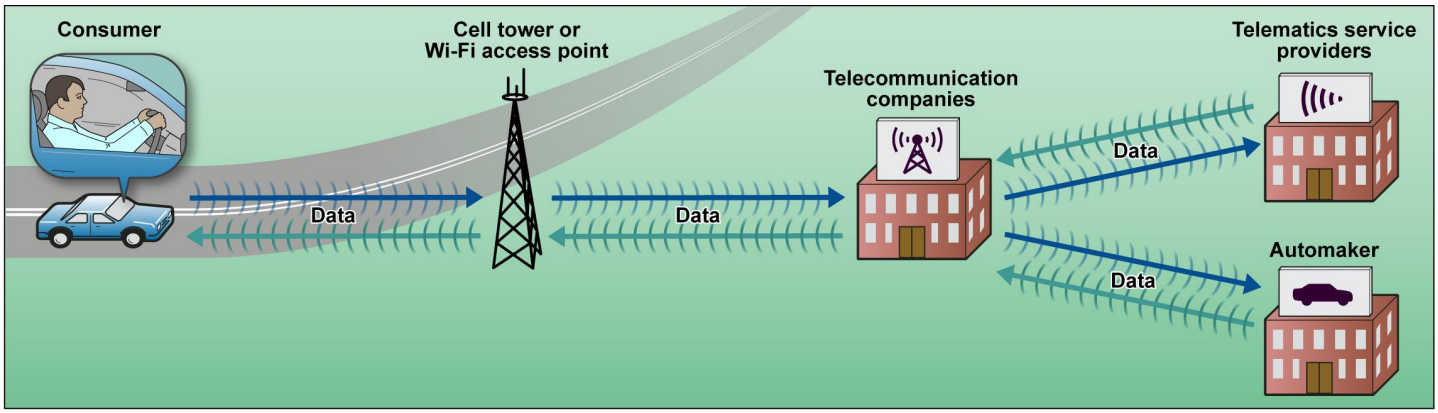
Background

Connected vehicles offer services and features to consumers through wireless communication systems. Technologies, such as in-vehicle sensors and global positioning systems, generate data that are transmitted through two-way communication between a vehicle and a central computer system or a call center. As shown in figure 1, automakers use third parties to provide connectivity[16] (e.g., enable a vehicle to transmit and receive voice and data communications) and typically contract with third parties to provide support for the services offered in connected vehicles ("connected vehicle services"). For example, automakers may contract with:

- telecommunication companies to connect a vehicle to the internet or a wireless network,
- telematics service providers to provide connected vehicle services by staffing calling centers and processing data, and
- content providers to provide optional applications, similar to those available on a smartphone, that consumers can access through their vehicle's console.

[16]Connectivity may be provided through a subscriber identity module—SIM—card and modem embedded in the vehicle. Connectivity may also be provided through a consumer's smartphone. In this case, the consumer's smartphone must be in the vehicle, and data are transferred or received using the consumer's cellular data plan.

Figure 1: How Data Are Transmitted to Provide Connected Vehicle Services



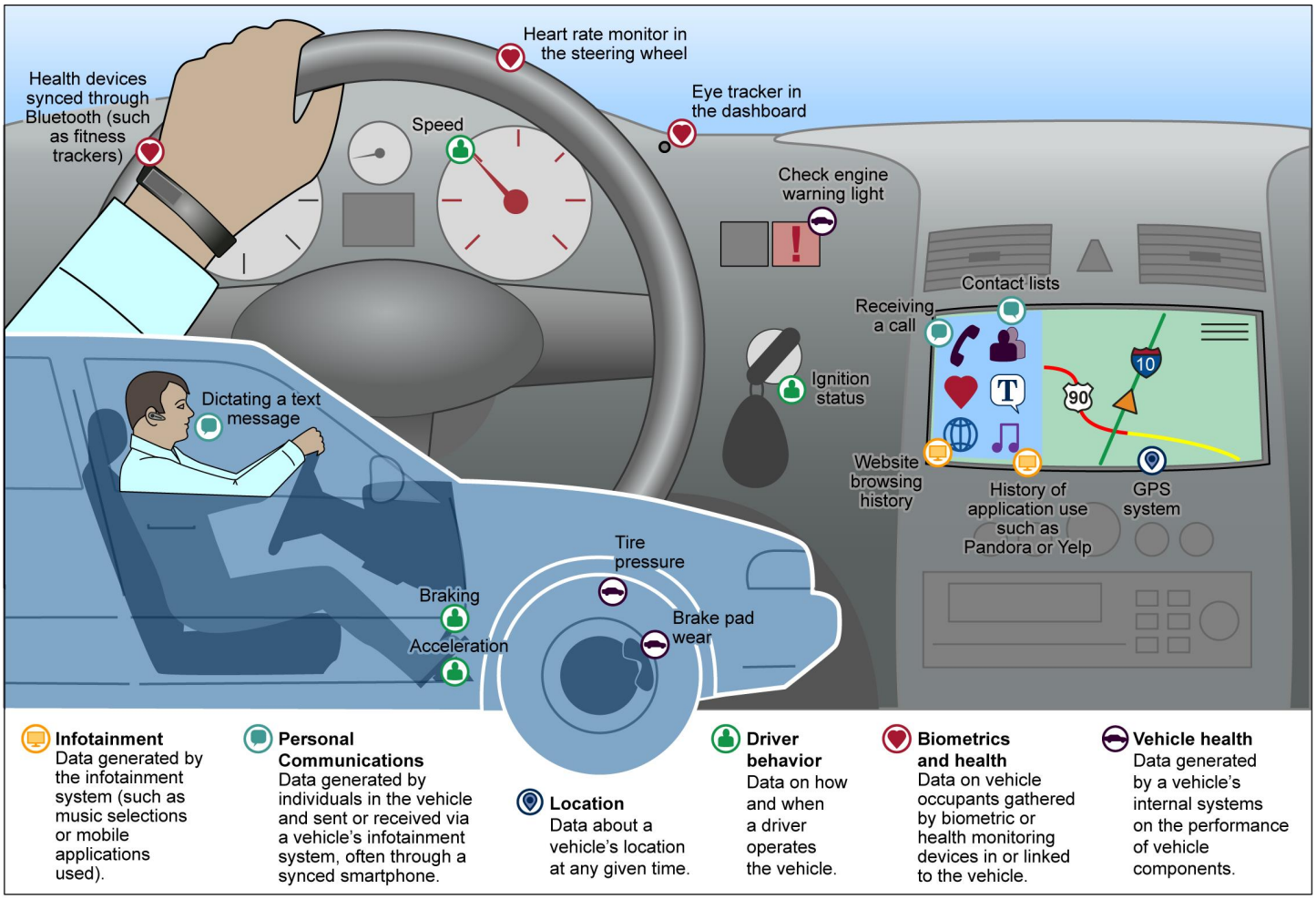
Source: GAO. | GAO-17-656

Connected vehicles can offer consumers a range of safety, security, and convenience services.[17] For example, roadside assistance and automatic crash notification services allow for voice and data communication between a vehicle and a person at a call center. In providing these services, connected vehicles generate, transmit, and receive various types of data, such as a car's location. In this report, we categorized data that are collected or that could be collected by connected vehicles into six categories as defined and described in figure 2.[18]

[17]Many new vehicles also offer advanced driver assistance systems, such as blind spot warnings, collision warnings, and parking assistance. These safety features, while often found in vehicles with connected vehicle services, do not require a wireless connection nor do they typically transmit data in order to function properly. Due to this distinction, we do not classify these as connected vehicle services.

[18]We used data categories similar to those used in P. Lawson, B. McPhail, and E. Lawson, *The Connected Car: Who is in the Driver's Seat? A Study on Privacy and Onboard Vehicle Telematics Technology* (Vancouver, British Columbia: British Columbia Freedom of Information and Privacy Association, 2015), accessed April 19, 2016, https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/CC_report_lite-1v2.pdf. While the focus of our report is the collection, use, and sharing of connected vehicle data by automakers, other parties can record and collect data from vehicles. For example, aftermarket telematics service providers and insurance companies can collect data on location, vehicle health, or driver behavior.

Figure 2: Definitions and Examples of How Connected Vehicles Generate Different Types of Data



Sources: British Columbia Freedom of Information and Privacy Association, and GAO. | GAO-17-656

Note: This figure summarizes connected vehicle data categories and data elements presented in P. Lawson, B. McPhail, and E. Lawson, *The Connected Car: Who is in the Driver's Seat? A Study on Privacy and Onboard Vehicle Telematics Technology* (Vancouver, British Columbia: British Columbia Freedom of Information and Privacy Association, 2015), https://fipa.bc.ca/wordpress/wp-content/uploads/2015/05/CC_report_lite-1v2.pdf.

Personal information includes identifying information such as a consumer's name, address, e-mail or other information that directly links back to an individual as well as other information that can be reasonably

linked to a specific consumer, computer, or device.[19] For example, in the connected vehicle context, data (e.g., GPS coordinates or airbag status) that can be linked to a vehicle owner is often treated as personal information. Personal information collected from vehicles varies in its sensitivity. As reported by FTC staff, some personal information, such as data on precise geolocation, is considered sensitive due to what it can reveal about someone (e.g., routines).[20]

There is no federal comprehensive privacy law governing the collection, use, and sale of personal information by private sector companies. Rather, federal statutes and regulations addressing privacy issues in the private sector are generally tailored to specific purposes, situations, types of information, or sectors or entities. For example, the Health Insurance Portability and Accountability Act governs the use and disclosure of an individual's health information by certain entities. Federal law also does not require all companies to have a privacy policy or to notify consumers of their privacy practices. While no single federal agency oversees data privacy issues, FTC is a law enforcement agency with a mission to promote consumer protection and prevent business practices that are anticompetitive, deceptive, or unfair to consumers. The National Highway Traffic Safety Administration (NHTSA) within DOT is responsible for vehicle safety.

Many organizations and governments have used the Fair Information Practice Principles (FIPPs) to guide their privacy practices. The Organisation for Economic Co-Operation and Development developed a version of the FIPPs—a set of internationally recognized principles for protecting the privacy and security of personal information—in 1980 that has been widely adopted and was updated in 2013. While the FIPPs are principles, not legal requirements, they provide a framework for balancing privacy protections with other interests.[21] Like other industries, the

[19]This information is also called personally identifiable information. In 2015, we added protecting the privacy of this information by both federal and nonfederal entities to our high-risk list. See GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[20]FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Washington, D.C.: January 2015).

[21]The FIPPs address the collection and use of personal information, data quality and security, and transparency, among other things, and have served as the basis for many of the privacy recommendations federal agencies have made. For the full list of principles in the FIPPs, see appendix II.

automobile industry recently developed a set of privacy principles—the *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services ("Consumer Privacy Protection Principles")*. These principles are a self-regulatory framework influenced by the FIPPs and were adopted by most automakers with vehicle sales in the United States. The *Consumer Privacy Protection Principles* went into effect January 2, 2016.[22]

Selected Automakers Collect Different Types of Data from Connected Vehicles and Reported Limited Use and Sharing

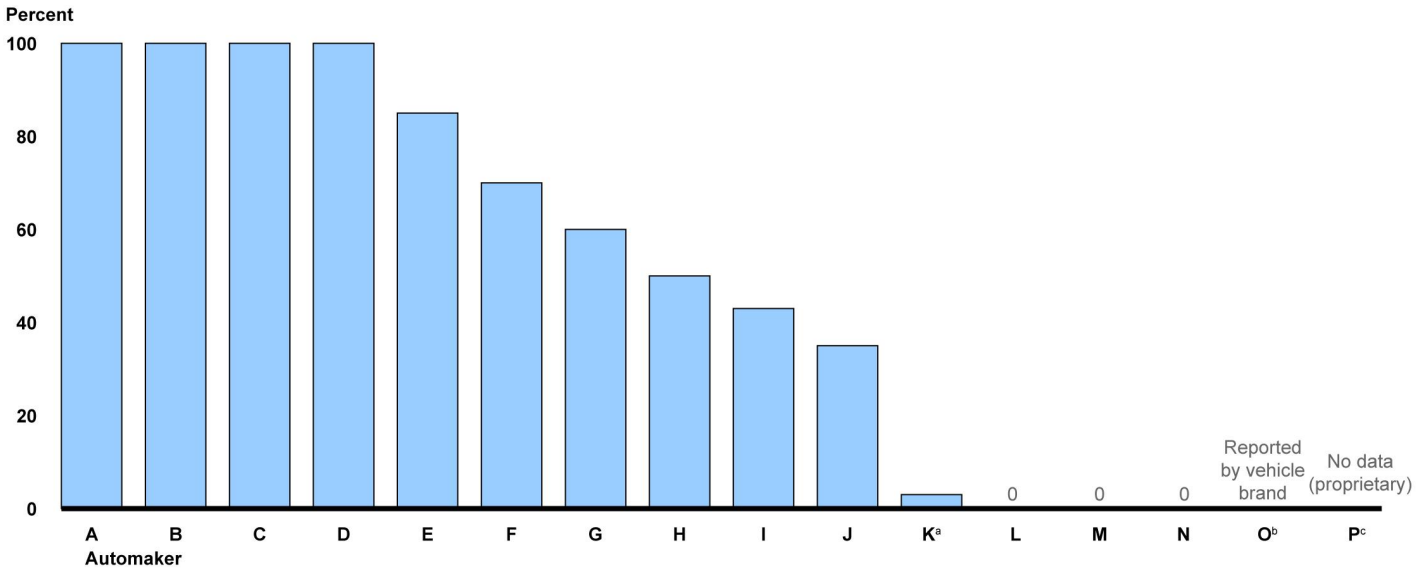
Availability of Connected Vehicles Varies, but Selected Automakers Plan to Increase Offerings

Nearly all selected automakers offer connected vehicles or plan to offer them in the next 5 or more years. Specifically, 13 of the 16 automakers we interviewed sell new vehicles that met our definition of a connected vehicle—ones that come equipped with technologies and services that transmit and receive data wirelessly (see fig. 3).[23] Four of these automakers currently provide connected services in all of their vehicles; most of the remaining automakers reported increases in their production of connected vehicles over the last 5 years.

[22]For the full list of principles in the *Consumer Privacy Protection Principles*, see appendix II.

[23]For this review, new vehicles are those sold in the most recent model year.

Figure 3: Selected Automakers' Reported Model Year 2017 Offerings of Connected Vehicles



Source: GAO analysis of interview responses. | GAO-17-656

[a]Percentage shown in figure is for model year 2016 vehicles.

[b]Automaker representatives provided the percentage of connected vehicles offered by vehicle brand, not for the automaker as a whole.

[c]Automaker representatives did not provide the percentage of connected vehicles offered, but reported that the automaker offers connected vehicles.

Of the 12 automakers we interviewed that do not currently offer connectivity in all of their new vehicles, all but 1 told us they plan to do so. Three plan to offer all connected vehicles in the next 3 to 4 years, and 8 plan to offer all connected vehicles in 5 or more years. Several automakers noted that consumer demand will influence when they will offer all connected vehicles.

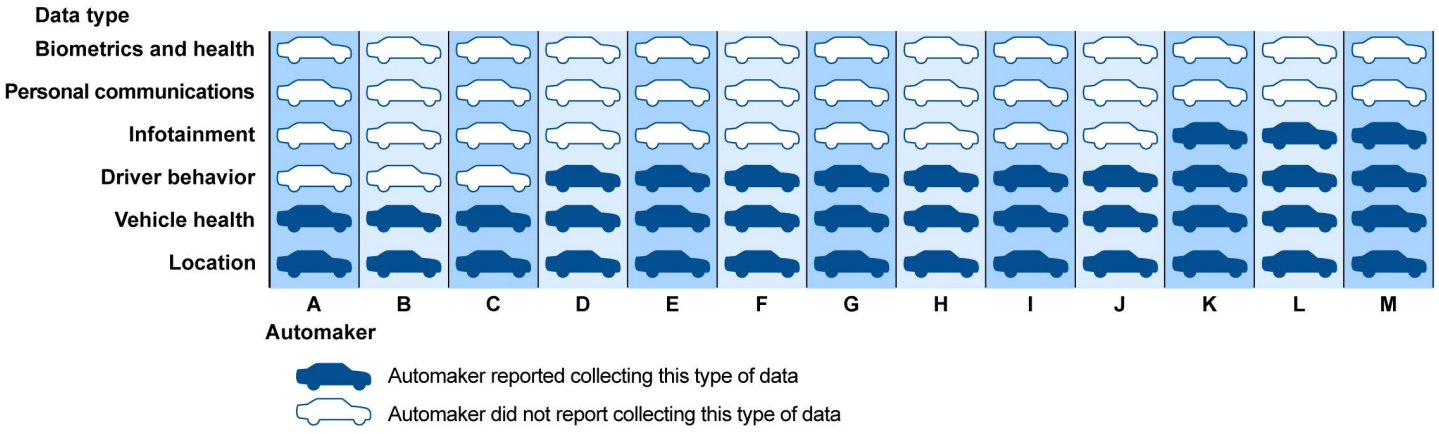
While most automakers offer connected vehicles and services, not all consumers with access to these services use them. Based on our interviews with automakers, the percentage of customers who use these services ranges from less than 50 percent up to 100 percent. Selected automakers differed in how they offer these services to consumers. For example, some automakers offer free trials for 3 months, 6 months, or 1 year, while other automakers offer these services at no additional cost.

The 3 automakers that do not offer connected vehicles or connected vehicles services told us they do not collect any data from their vehicles.[24] Our discussion below focuses on the 13 automakers that offer connected vehicles and services.

Collected Data Include Location, Vehicle Health, Driver Behavior, and Infotainment Data

Based on interviews with the 13 selected automakers that offer connected vehicles, the types of data they collect from those vehicles vary. All 13 reported collecting vehicle health and location data (see fig. 4). However, fewer automakers reported collecting driver behavior and infotainment data, such as music selections and mobile applications used. These 13 automakers did not report collecting data related to vehicle occupants' health or personal communications.[25]

Figure 4: Types of Data Collected by Connected Vehicles as Reported by 13 Selected Automakers



Source: GAO analysis of intervew responses. | GAO-17-656

[24]One of these automakers offers a remote start application consumers can buy as an aftermarket device that collects some data, but it does not offer connected vehicle services or consider its vehicles to be connected.

[25]The two telecommunications companies we interviewed told us they do not collect data from connected vehicles when contracted by automakers to provide connectivity to vehicles. The one telematics service provider we interviewed confirmed that when contracted to provide connected vehicle services for automakers it collects certain types of data (at the direction of the contracting automaker) to enable the provision of the contracted services.

Selected Automakers Reported Using Collected Data Primarily to Provide Services to Consumers and for Research and Development

According to the 13 selected automakers that offer connected vehicles, they currently use data collected from connected vehicles to provide connected vehicle services, and some use the data for research and development and marketing.

- *Connected Vehicle Services*: According to all of these 13 automakers, collected data are used to provide services, such as automatic crash notification or roadside assistance, to customers. Providing these services typically requires location, vehicle health, and for some services, driver behavior data. For example, sensors in a connected vehicle may detect that an airbag deployed. The connected vehicle transmits this information to the automaker or the provider operating the automatic crash notification service. The provider uses a vehicle's location, status of airbag deployment, rollover status, and other pertinent information to inform and request assistance from emergency responders.
- *Research and Development*: All but 1 of these 13 automakers told us they also use collected data for research and development, specifically to improve their vehicles' safety and performance.[26] For example, automakers may use vehicle health data (e.g., diagnostic trouble codes) to identify an issue with a certain model or component within their vehicles. Twelve of these 13 automakers also told us they use these data to improve connected vehicle services they offer. For example, these collected data allow them to see which services or features consumers actually use and how they use them.
- *Marketing*: Five of these 13 automakers reported using collected data to market products and services to consumers, for example using vehicle health data to target advertisements to specific consumers for specific vehicle service or maintenance offers.

These 13 selected automakers differed on who owns data collected from their connected vehicles. Specifically, 7 told us ownership of these data is

[26]The automaker that reported not using connected vehicle data for research and development or product improvement told us they do not use data that can be linked back to a vehicle for this purpose, but use de-identified data for additional purposes.

legally unclear or they do not yet have a position.[27] Of the remaining automakers, 3 said the vehicle owner owns the data, but the automaker has a license to use them; 2 said the automaker owns the data, and 1 said the automaker owns anonymized data and the customer owns personal data (e.g., data tied to a vehicle identification number). As we reported in 2016, data ownership is a potential challenge to achieving gains in transportation safety and efficiency.[28] In the context of connected vehicles, data ownership can determine who or what entity controls access to the data and how they can be used.[29]

Selected Automakers Reported Sharing Data on a Limited Basis

All 13 selected automakers that offer connected vehicles said they typically do not share collected data with unaffiliated third parties. For example, none of these automakers reported sharing collected data with firms that collect and sell information (data brokers).[30] When automakers do share collected data, they said they typically do so with explicit consumer consent, at the request of a consumer, or to comply with a valid court order. Specifically, all of these automakers said they would share collected data with law enforcement in response to a valid court order or in exigent circumstances. Seven automakers said they share collected data, specifically vehicle health data, with dealerships to aide in vehicle

[27]For the purposes of our report, we have excluded event data recorder data. The Driver Privacy Act of 2015, a subtitle of the Fixing America's Surface Transportation Act of 2015 ("FAST Act"), established that any data retained by an event data recorder is the property of the owner of the motor vehicle, or in the case of a leased vehicle, the lessee of the motor vehicle. Pub. L. No. 114-94, Title XXIV, Subtitle C, § 24302(a), 129 Stat. 1312, (2015). The FAST Act also established that a court or other judicial or administrative authority may access this data in certain cases. Pub. L. No. 114-94, Title XXIV, Subtitle C, § 24302(b)(1)(A).

[28]See GAO-16-659SP.

[29]For more information on data ownership in this context, see J. Zmud, M. Tooley, and M. Miller, "*Data Ownership Issues in a Connected Car Environment: Implications for State and Local Agencies*" (College Station, TX: Texas A&M Transportation Institute, November 2016), accessed March 15, 2017, https://tti.tamu.edu/publications/catalog/record/?id=44273

[30]For more information on information resellers and the related privacy issues, 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).

servicing.[31] Two automakers reported sharing collected data with insurance companies to enable consumers to participate in insurance plans that base premiums on driving behavior. Several automakers reported sharing and using collected data that has been de-identified more widely than they do data that can be linked back to a vehicle or vehicle owner. For example, one automaker discussed sharing de-identified vehicle health data with university-based researchers to examine vehicle structural integrity after crashes. Other automakers mentioned sharing de-identified location data with traffic services to improve their accuracy. Some automakers we spoke with emphasized that their current use and sharing of data may change as the industry evolves and data collection expands.

Selected Automakers' Reported Policies Partially Reflected Leading Privacy Practices Relevant to Connected Vehicle Data Privacy

Automakers' Reported Policies Partially Reflected Six Identified Leading Practices

As mentioned above, for the purposes of this report we identified six leading practices most relevant to connected vehicle data privacy, based on our analysis of the FIPPs and other policy frameworks (see table 1).[32]

[31]We asked all automakers about sharing data with dealerships; however, two did not respond to this question.

[32]Reports used in our leading practice analysis include: (1) Organisation for Economic Co-operation and Development, *The OECD Privacy Framework* (July 11, 2013 revision) *(*known as the *"Fair Information Practice Principles")*; (2*)* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012); (3) FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (2015); (4) NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety (*2016); and (5) National Institute of Standards and Technology, *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems* (2017).

Table 1: Leading Privacy Practices Identified as Relevant to Connected Vehicle Data for the Purposes of This Report

Leading practice	Description
Transparency	Provide consumers with understandable and accessible information about privacy practices, including information that specifies the types of personal data collected; why such data are needed; how data will be used; and whether and for what purpose(s) data will be shared with third parties.
Focused data use[a]	Provide reasonable limits on personal data collected and retained, including collecting only as much personal data as needed to accomplish specific purposes; using de-identified data to the extent possible; and securely disposing of data once no longer needed. Consumers also have a right to understand the limits that the respective company sets as part of its privacy policy.
Data security	Maintain reasonable safeguards to control risks related to data—such as loss, unauthorized access, use, destruction or modification, and improper disclosure—and take associated steps including conducting risk assessments.
Data accuracy and access	Allow consumers to access and correct their personal data, and use reasonable measures to ensure personal data is accurate.
Individual control	Allow consumers to control what personal data companies collect from them and how these data are used. Further, companies should offer clear and simple choices, presented in ways that enable consumers to make meaningful decisions about data collection, use, and sharing.
Accountability	Handle data with appropriate measures, including holding company employees responsible for adhering to the company's privacy principles and requiring third-party recipients of data to adhere to those same principles.

Source: GAO analysis of privacy frameworks. | GAO-17-656

[a]This leading practice relates to two principles from the FIPPs framework: (1) Collection limitation: limiting the data collected, and only collecting this data if the individual's consent has been obtained by lawful and fair means; and (2) Use limitation: not sharing personal information or using it for other than a specified purpose without the consent of the individual.

To assess the extent to which selected automakers' reported privacy policies reflected each leading practice, we identified multiple elements for each practice. We then reviewed selected automakers' written privacy notice(s) and their responses to interview questions about their privacy practices. We did not evaluate the extent to which selected automakers follow their reported privacy policies.[33] Although the leading practices are interrelated, we focused our assessments on how fully the automakers' practices met each leading practice.

We found that most selected automakers' reported privacy policies at least partially reflected each of the six identified leading practices.[34]

[33]This was not a compliance review of automakers. As leading practices, these are not legally binding. See appendix I for more details about our scope and methodology, and appendix III for more details about how we conducted this privacy policy analysis and for a description of the results.

[34]We determined how fully an automaker reflected each practice using three categories: *substantially reflected* the practice*, partially reflected*, and *minimally reflected*.

Although we saw some variation among automakers, they tended to reflect and not reflect the same leading practice elements. For example, most automakers reported limiting the sharing of data and using safeguards to protect data security. However, none of the automakers' written notices were in plain language, and their reported data collection, use, and sharing practices generally were more limited than suggested in their notices. Automakers reported obtaining consent before collecting data from vehicles, but they offered few options besides *opting in* and *opting out* of sharing data.

Transparency: All 13 selected automakers' written privacy notices were readily accessible from their public websites, but based on our analysis, none of the notices was clearly written.[35] As we have previously reported, FTC and others have recommended that privacy notices should be *readily accessible, clearly written, and describe all the purposes for which personal data are collected and shared*.[36] All of the automakers' notices discussed the types of data collected; the potential purposes for collecting the data, such as to provide the connected services; and some conditions when data might be shared with third parties. However, none of the notices was written in plain language, a lack that could make them difficult for consumers to understand. In addition, most notices did not describe all of the types and purposes of the connected vehicle data that were being collected, but instead used broad language to describe this process. For example, of the 15 notices, only 2 included a list with all of the *actual* purposes for which the automaker collects data, and only 1 included a list with *all* of the types of personal data collected.[37] Two notices clearly stated that the purposes identified for data collection were not exhaustive.

[35]Readability was judged using *Flesch Reading Ease* scores. Scores fall on a scale from 0 to 100, with 0 being nearly impossible to read and 100 being simple enough for a fifth grader to read. A score of 60 or above qualifies as "plain language." The formula is based on average sentence length and average word length. The version we used was included in the Microsoft Word processing software. As GAO has previously reported, the *Flesch Reading Ease* score is one of the most widely used, tested, and reliable formulas for calculating readability. See GAO-16-750, *Equal Employment Opportunity: Strengthening Oversight Could Improve Federal Contractor Nondiscrimination Compliance* (Washington, D.C.: September 2016).

[36]See GAO-14-81.

[37]As noted previously, 13 automakers in our selection offer connected vehicle services. Throughout this discussion, when we refer to automakers, we mean those offering such services. However, one of these 13 automakers has different written privacy notices and reported privacy practices for its three affiliated brands. As a result, our analysis of automakers' privacy policies was done on 15 sets of privacy policies.

Although the use of broad language is common for privacy notices and is not specific to the auto industry, it does not promote transparency. Several automakers discussed their other efforts to increase transparency. For example, one automaker reported revising its website to offer a consumer-friendly privacy portal after signing onto the *Consumer Protection Privacy Principles*. Three other automakers told us that they display their privacy policies on in-vehicle displays. Two automakers told us that a recently issued consumer guide could help promote understanding about this issue. In January 2017, the National Automobile Dealers Association and Future of Privacy Forum issued a consumer guide outlining types of vehicle data, practices governing their collection and use, and potential consumer options; the guide is to be available at auto dealerships.[38]

Focused Data Use: Most selected automakers reported limiting their data collection, use, retention and sharing, but their policies varied. Most written notices did not clearly identify data sharing and use practices. In interviews, all 13 selected automakers reported limiting the data collected from connected vehicles, with some (4 of 13) noting that they only collect the specific data they need to provide the consumer with services. With regard to data use, as discussed previously, all 13 automakers reported they use collected data to provide direct consumer services, such as roadside assistance, but some automakers (5 of 13) reported they use such data for marketing other services. Also, all 13 automakers told us that they use de-identified data when possible, such as when the data are being used for research and development purposes.[39] Most automakers (12 of 13) also told us that they limit data retention, but policies varied.[40] For example, of the 12 automakers that limit retention, 8 told us that their retention time frames depend on the type of data, while one of them specified that it retains all connected vehicle data for 6 years regardless

[38]National Automobile Dealers Association and Future of Privacy Forum, "Personal Data in Your Car," Jan. 25, 2017.

[39]As we have previously reported, by using de-identified data (from which the personally identifiable information has been removed) companies can decrease the privacy risks to consumers that their data will be used for purposes that they do not expect or did not agree to. See GAO-14-81.

[40]The remaining automaker, explained that it is still developing its retention policy. As we have previously reported, longer retention periods put data at increased risk for unauthorized access or accidental disclosure, and some recommended practices state that privacy policies should specify the time frame for retaining consumer data. See GAO-14-81.

of data type. Two automakers also told us that they are still developing their policies, so their retention time frames may change. With regard to data sharing, as mentioned previously, all 13 automakers told us that they do not typically share collected data with unaffiliated third parties. However, most automakers' written privacy notices used vague language and did not consistently reflect their relatively limited data collection, use, retention, and sharing. For example, none of the notices stated that the automaker would not use data for reasons other than those listed in the policy, and only one notice specified the automaker's data retention time frame. In another example, less than half of the notices (6 of 15) stated that data would not be shared with or sold to non-affiliated third parties, such as data brokers. Similarly, less than half of the notices (7 of 15) stated that location and driving behavior data would not be shared with any parties besides service providers without first obtaining the consumer's consent. Only 2 notices included both of these statements about sharing.

Data Security: Selected automakers reported using various methods to safeguard data, including methods that we have reported could be applied to increase vehicle data security. As we reported in 2016, automakers can identify and mitigate cybersecurity vulnerabilities by using practices such as conducting risk assessments and by employing technological measures.[41] In interviews, all 13 automakers reported using policy and technological measures to protect data, such as limiting data access to certain company staff, using firewalls and encryption,[42] and using "penetration testing" and "code reviews."[43] In addition, 12 automakers told us that they participate in the Auto-Information Sharing and Analysis Center, an industry-operated forum that includes automakers and parts suppliers. The center seeks to heighten awareness and increase security by allowing industry stakeholders to share threat information and potential mitigation strategies. Most automakers (9 of 13) also reported conducting privacy risk assessments, which would involve determining, among other things, the sensitivity of the collected data and

[41]See GAO-16-350.

[42]A firewall is a system that controls and limits communication between two or more networks. Encryption protects data through a process of transforming ordinary data into code form so that the data are unintelligible to users without the proper decryption key.

[43]"Penetration tests" seek to simulate real-world vehicle cyberattacks in an attempt to identify ways to circumvent and defeat the vehicle's cybersecurity protections. "Code reviews" seek to systematically examine the vehicle's software code so that any mistakes that were overlooked in the initial development phase can be addressed.

the potential risks if the data were improperly lost, accessed, or disclosed.[44] In addition, almost all of the notices (14 of 15) explained safeguards used to protect data, and some (7 of 15) also included examples of industry standard practices used for data security.

Data Access and Accuracy: Selected automakers reported offering consumers various methods to access their personal account information, but most of their notices were unclear about methods used to ensure data accuracy. The majority (9 of 13) of automakers told us that consumers can access and correct information, such as name and address, related to the driver or subscriber.[45] For example, 5 of these automakers noted that such subscriber information can be accessed through websites or mobile applications. One other automaker told us that consumers can access information on the website or mobile application but must e-mail or call the automaker to correct it. For other types of vehicle data—such as location, vehicle health, and driver behavior—consumers' access varied among automakers. For example, some (4 of 13) automakers reported that consumers can access their vehicle health data—such as tire pressure information—through websites or mobile applications. On the other hand, 2 automakers told us it is not possible for consumers to access any data other than subscription-related data. With regard to data accuracy, the majority (9 of 13) of automakers told us they take steps, such as validation tests and other quality control measures, to ensure the accuracy of data collected from connected vehicles.[46] Although most (12 of 15) notices explained how to access and correct one's data, only a few notices (4 of 15) discussed actions the company takes to ensure data accuracy.

Individual Control: Selected automakers reported that they obtain explicit consent before collecting data and most seek consent again, but they offered few options to consumers besides *opting into* sharing data and receiving the connected services or *opting out* of the service entirely if they do not wish to share data.[47] In interviews, all 13 automakers told us

[44]Of the remaining 4 automakers, 3 did not answer this question, and one indicated that it does not currently conduct privacy risk assessments yet but may do so in the future.

[45]The remaining 4 automakers did not answer this question.

[46]The remaining 4 automakers did not answer this question.

[47]Although most automakers reported only giving consumers the choice between *opting in* and *opting out*, 3 automakers told us they allow consumers to opt out of sharing some types of data without losing access to all services. For example, one automaker told us that while some minimum data sharing is necessary for receiving 'core' connected

that they obtain explicit consent before initiating services that require data to be collected and transmitted, typically through the consumer signing a service agreement or activating the service. Also, the majority of automakers (8 of 13) seek consent again in certain circumstances (e.g., when updating a service subscription or if the company's data use practices will change significantly). In addition, most of the notices (13 of 15) discussed consumer choices, including how to opt out of sharing data with the automaker. However, all 13 automakers told us while consumers can opt out of sharing data this would typically involve losing all connected vehicle functionality, in part because connected vehicle services are often bundled.

Accountability: Selected automakers reported using various methods to ensure that their staff and third parties receiving personal data handle them properly and most automakers' notices discussed the methods used. In interviews, almost all automakers (12 of 13) reported that they work to ensure that third parties receiving data meet certain requirements, such as following the automaker's privacy policies, and most reported including data-handling requirements in their contractual agreements.[48] Several also reported imposing additional requirements, such as asking third parties to conduct privacy risk assessments. Nine automakers also reported that they conduct risk assessments related to third parties' use of data collected from connected vehicles. Most automakers' notices included descriptions of the methods used to promote accountability and designated which entity is ultimately responsible for properly handling data. For example, almost all notices (14 of 15) named the company responsible for handling personal data and provided contact information. In addition, the majority of notices (9 of 15) outlined requirements that third parties must meet before receiving data.

Privacy Notices Do Not Guarantee Privacy Protections

Views differ on the importance and effectiveness of privacy notices in providing privacy protections for consumers. For example, FTC's 2012 report recommended that companies should provide easy-to-use choice mechanisms that allow consumers to control whether their data are

services—such as roadside assistance and crash response—consumers may opt out of sharing other data and forego other services such as Wi-Fi and hands-free calling.

[48]The remaining automaker did not answer this question.

collected and how they are used;[49] such mechanisms could include privacy notices. In the report, FTC also recommended that privacy notices should be made clearer, shorter, and more standardized to increase consumers' ability to comprehend and compare various companies' data practices. Most (14 of 16) selected experts in our review agreed with that FTC recommendation.

However, FTC, we, and others have acknowledged that improved notices alone cannot guarantee consumer protections. Specifically, FTC has argued that clearer notices and improved consumer choices would need to be combined with other privacy practices, such as focused data collection and data security, to provide substantive privacy protections for consumers. Furthermore, FTC stated that when combined, such practices would help accomplish a broader goal of shifting the burden for protection away from consumers and to the companies handling consumer data.[50] We have also reported that notices alone do not guarantee consumer protections. For example, as we reported in 2016, some consumers do not take the time to read notices, decreasing their ability to provide fully informed consent.[51] In another example, four experts in our review mentioned the multiple decisions and corresponding large amount of paperwork required for buying a vehicle as factors that would make it less likely for a consumer to thoroughly read the privacy notice.

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

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

[51]See GAO-16-659SP and GAO-04-280, *Consumer Protection: Federal and State Agencies Face Challenges in Combating Predatory Lending*, (Washington, D.C.: January 2004).

Selected Experts Had Concerns about Connected Vehicle Data Privacy and Automakers' Privacy Efforts

Selected Experts Generally Agreed Broader Privacy Concerns Applied to Connected Vehicle Data

In interviewing selected experts on privacy issues related to connected vehicle data, we presented the experts with general privacy concerns about the commercial collection and use of data that we had identified from our and other federal agencies' reports[52] and interviews with organizations that advocate the protection of the privacy of consumers' data and asked the experts if these issues applied to data collected through connected vehicles. A majority of the experts generally agreed that these general data privacy issues, as described in table 2, apply to connected vehicle data.

[52]See, for example, GAO, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law,* GAO-15-621 (Washington, D.C.: July 30, 2015) and FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Washington, D.C.: January 2015).

Table 2: Selected Experts' Views on Consumer Privacy Issues Related to Data Collected through Connected Vehicles

Privacy issue	Description	Number of selected experts who agreed issue is relevant to connected vehicles
Tracking	*Information could be used to track individuals across locations without their knowledge or consent.*	16 of 16 experts
Loss of consumer control over personal information	*Information could be used, shared, or sold in ways that consumers do not understand, anticipate, or consent to.*	16 of 16 experts
Insecure data	*Information could be subject to data breaches that could increase possibility of identity theft, harassment, and stalking.*	16 of 16 experts
Lack of sufficiently informed consent: low consumer awareness	*Consumers may not read or fully understand the end-user agreements and/or privacy statements.*	15 of 16 experts
Disparate treatment	*Information could be used to treat consumers differently or consumers that decline consent could be treated differently.*	13 of 16 experts
Lack of sufficiently informed consent: lack of company transparency	*Privacy policies/statements may not be written clearly and/or may disclaim as much as possible to avoid action by the Federal Trade Commission.*	13 of 14 experts[a]
Little or no consumer choice about privacy	*Consumers must consent to share data as a condition of use or lose access to the service or technology.*	13 of 15 experts[a]

Source: GAO analysis of selected experts interview responses. | GAO-17-656

[a]Not all experts responded to all questions.

All selected experts agreed that tracking, loss of consumer control over personal information, and potentially insecure data were relevant privacy concerns. They emphasized that using location data to track individuals is particularly relevant in the context of vehicles.[53] For example, one expert said location data could paint a picture of an individual's life, revealing with whom they associate, the doctors they see, and the places they frequent.[54] Experts also raised concerns about potentially inappropriate or illegal uses of location data, such as stalking. All experts expressed concern about potential data access through a security breach; however, no one we interviewed, including automakers, selected experts, industry groups, or government officials was aware of an incident where a database storing connected vehicle data had been compromised

[53]In 2016 the Pew Research Center reported that, as consumers considered scenarios where they would exchange personal data about themselves for something considered of value (such as access to a useful service), sharing location data was especially sensitive and elicited some of the most strongly negative reactions. See L. Rainie and M. Duggan, Pew Research Center, *Privacy and Information Sharing*, December 2015, accessed March 24, 2017, http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/.

[54]We previously reported on privacy concerns with location data for in-car, location-based services, which are among the systems available in connected vehicles. See GAO-14-81.

maliciously.[55] Regarding loss of consumer control over personal information, one expert explained that it is not possible for a consumer to know exactly what is collected, when, and how the data are used. Another expert noted that other technologies face this same challenge; however, consumers may be less aware of what their vehicle is doing than their computer or smartphone. In addition, vehicles may be used by multiple individuals, and one expert expressed concern about how multiple drivers of a car would be informed about data collection. Some experts thought data sharing and third-party use could become a greater issue as the auto industry evolves. These issues mirror concerns we reported on in 2013 and 2015 about the collection, use, and sharing of personal data by commercial entities.[56]

The majority of experts we interviewed also agreed that the lack of sufficiently informed consent (due to low consumer awareness and lack of company transparency), disparate treatment, and little or no consumer choice were relevant privacy concerns. Several experts said that, as in other industries, informed, meaningful consent is difficult to obtain, as consumers may not read notices and automakers may not present privacy information clearly. Regarding disparate treatment, two experts raised the example that data from connected vehicles could potentially be used to treat consumers differently, and unfairly, in the provision of auto insurance.[57] Finally, experts raised concerns about consumer choice. For example, as described above, several experts noted that consumers must provide consent to all data collection and use or not receive any services. Another expert said that consumers have limited choice because vehicles are essential to people's lives. Similarly, another expert noted that it is difficult to compare privacy practices across automakers and connected

[55]Fifteen selected experts were not aware of incidents of databases storing data extracted from connected vehicles being compromised; two experts had expressly looked for such incidents. One expert noted an incident where a design issue enabled vehicle data to be accessed on the web (manufacturer coding error); however, this was not an example of a database being compromised with malicious intent.

[56]GAO-13-663 and GAO-15-621.

[57]For example, an expert explained that factors such as working a night shift or living in a neighborhood with pothole-ridden roads could affect driving behavior and insurance rates. See also Electronic Privacy Information Center, *Testimony and Statement for the Record of Khaliah Barnes on "The Internet of Cars",* Joint Hearing before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittee on Information Technology and Subcommittee on Transportation and Public Assets (Washington, D.C.: November 18, 2015), accessed June 17, 2016, https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf.

vehicle platforms and that consumers cannot easily change their minds after buying a car, as it is a large financial investment.[58]

Majority of Selected Experts Expressed Concern about Automakers' Privacy Policies and Efforts

While we did not ask selected experts to comment on individual automaker policies, some were concerned about automakers' efforts to protect consumer privacy. As previously discussed, automakers signed onto the *Consumer Privacy Protection Principles* to demonstrate their commitment to protect consumers' privacy. However, the majority of experts we interviewed (13 of 16) did not think that these principles provide sufficient guidance to inform automakers' actions or protect consumers' privacy.[59] Some experts noted that other industries, such as the credit card industry, have developed more specific self-regulatory guidelines that include enforcement measures and better protect consumers.

Most selected experts said the *Consumer Privacy Protection Principles* lacked specificity about, for example, data use and consumers' right to protection. For example, they said the principles used "vague language" and allowed for data use without consumers' affirmative consent for "legitimate business purposes," which are not clearly defined.[60] To remedy these issues, six experts said the *Consumer Privacy Protection Principles* should be more specific, and four said the principles should define restrictions on data use. Most experts we interviewed agreed automakers should limit data retention (13 of 16) and limit data collection (12 of 16).[61] While the majority of experts thought that automakers should de-identify data (11 of 15) for focused data use, four experts expressed skepticism about this practice, including whether it is possible to

[58]Experts raised additional concerns specific to connected vehicles; for example, one expert was concerned about the use of data taken from vehicles' external-facing cameras, and another expert was concerned that health data collected by vehicles would not be covered by any federal health privacy regulations.

[59]Two experts were not sure, and one expert said the principles provide sufficient guidance.

[60]Some experts specifically referred to the phrase "legitimate business purposes," which companies often use in privacy notices.

[61]Of those who did not agree with data retention and collection limits, two experts specifically cited the safety benefits of collecting vehicle data.

completely de-identify data. In 2013, we reported concerns about de-identifying location data. Specifically, we found that some methods of de-identification can allow for an individual to be re-identified, and that different de-identification methods and data retention practices may lead to varying levels of consumer protection.[62]

Other suggestions to improve the *Consumer Privacy Protection Principles* included making the principles enforceable,[63] making privacy information accessible and transparent, explaining the rationale or risks and benefits of data use, and laying out the trade-offs for consumers. All selected experts agreed that automakers should be required to obtain explicit consent for the use of sensitive data or data used in a manner beyond a consumer's expectations. In addition, the majority of experts we interviewed (13 of 16) agreed that automakers should obtain consumer consent at the time and in the context in which consumers are making a decision about their data. Several experts said that consumers should have access to personal data collected about them. However, auto industry trade association officials said that the *Consumer Privacy Protection Principles* provide automakers with a sufficient framework to address privacy issues and allow automakers the flexibility to tailor implementation.

[62]GAO-14-81. For more information on de-identification, see work by the National Institute of Standards and Technology and the Future of Privacy Forum, one of our selected experts. De-identification, while not perfect, is a significant technical control that may protect individuals' privacy (see National Institute of Standards and Technology, *NISTIR 8053: De-Identification of Personal Information* (October 2015), accessed October 18, 2016, http://dx.doi.org/10.6028/NIST.IR.8053). The Future of Privacy Forum proposed categories for de-identified data based on identifiers and an organization's safeguards and controls and proposed parameters for legal rules related to different categories of data. See J. Polonetsky, O. Tene, and K. Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification* (April 1, 2016). Santa Clara Law Review, Forthcoming, and Future of Privacy Forum, *A Visual Guide to Practical Data De-Identification* (Apr. 25, 2016), accessed June 14, 2017, https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/).

[63]One expert noted FTC's enforcement role, but did not think this step was sufficient. FTC's enforcement includes the ability to bring action against an automaker that violates the stated terms of its privacy policy.

FTC and NHTSA Have Efforts Related to Data Privacy Under Way, but NHTSA's Role Is Unclear

FTC and NHTSA Have Efforts and Guidance Related to Protecting Data Privacy

While no federal law expressly confers broad privacy protections for consumers' data and no single federal agency oversees data privacy issues, the FTC Act gives FTC the authority to bring actions against companies or individuals that engage in unfair or deceptive acts or practices in or affecting commerce.[64] According to FTC officials, the FTC Act applies to privacy and data security issues for connected vehicles. For example, FTC officials said they could use this authority to bring an action against an automaker that uses a consumer's data without his or her consent or in a way that violates the manufacturer's stated privacy policy. To date, FTC has not brought such a public enforcement action against a connected vehicle manufacturer or its affiliates, but it has brought such actions against other companies offering services in the Internet of Things. For example, in 2016, FTC settled a case alleging that critical security flaws in a company's routers put the home networks of hundreds of thousands of consumers at risk.[65] In addition, as the primary agency with authority over consumer privacy, FTC has ongoing efforts related to protecting the privacy of consumers that use connected devices in the Internet of Things, which includes connected vehicles. FTC and FTC staff have issued guidance, including two reports—*Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*[66] *and Internet of Things: Privacy and Security in a Connected World*[67]—both of which outline best practices for

[64]Section 5 of the FTC Act gives FTC the authority to initiate a civil proceeding when the FTC has reason to believe that a person, partnership, or corporation has been or is using an unfair method of competition or an unfair or deceptive act or practice. 15 U.S.C. § 45(a)(2).

[65]See FTC, *Privacy and Data Security Update 2016* (Washington, D.C.: January 2017).

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

[67]FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Washington, D.C.: January 2015).

companies. Prior to issuing these reports, FTC held outreach forums to gather views from a variety of stakeholders on these issues. One of these forums included a panel specifically focused on consumer-facing technology in connected vehicles, which covered, among other things, an overview of these technologies, security issues, and the diversity of auto industry practices.

NHTSA, according to agency officials, has broad authority over the safety of passenger vehicles and may issue voluntary guidance or mandate standards through a rulemaking process to address safety,[68] but it does not have the authority to regulate consumer privacy as it relates to motor vehicles or motor vehicle data. However, according to NHTSA officials, the agency is required to consider the privacy impacts of its regulatory activities. Specifically, NHTSA is required to conduct privacy impact assessments and inform the public about any consumer privacy impacts that may stem from its activities and the motor vehicle safety standards issued by the agency.[69] Also as part of the rulemaking process, NHTSA examines privacy as a component of public acceptance (i.e., will the public accept and use the mandated technology). According to NHTSA officials, this is an aspect of "practicability" the agency is required to consider when it proposes a motor vehicle safety standard under the Motor Vehicle Safety Act.[70] NHTSA may also address privacy in voluntary

[68]NHTSA issues Federal Motor Vehicle Safety Standards under the authority of the National Traffic and Motor Vehicle Safety Act, Pub. L. No. 89-563, § 103(a), 80 Stat. 718 (1966). In addition, NHTSA issues non-binding best practices, guidance and policies in furtherance of highway and motor safety under the general authority of 23 U.S.C. § 403 and 49 U.S.C. § 30182.

[69]Section 208 of the E-Government Act of 2002 requires federal government agencies to conduct a privacy impact assessment for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002). In addition, as required by the Consolidated Appropriations Act of 2005, federal agencies, including NHTSA, are required to assess and provide public notice of potential consumer privacy impacts that may stem from its activities. Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, § 522, 118 Stat. 2809 (2015). This act also requires federal agencies to conduct privacy impact assessments of proposed regulatory activities involving collections or systems of information in electronic form with the potential to impact individual privacy. Pub. L. No. 108-447, § 522.

[70]National Traffic and Motor Vehicle Safety Act, Pub. L. No. 89-563, § 103(a), 80 Stat. 718 (1966). According to NHTSA, the "practicability" of a motor vehicle safety standard involves a number of considerations, including whether the standard is technologically and economically feasible and whether the means used to comply with a standard will be accepted and correctly used by the public.

guidance it issues for technologies that it expects will have safety benefits and that it may regulate in the future.

Recent efforts by NHTSA to address emerging safety technologies align with NHTSA's goals of ensuring safety on the roadways and keeping pace with trends impacting consumers. These efforts also illustrate how NHTSA has addressed privacy issues related to emerging technologies. For example, in December 2016, NHTSA proposed a rulemaking on vehicle-to-vehicle technology[71] that, according to NHTSA, is expected to provide safety benefits. The proposed vehicle-to-vehicle rule involves the broadcast, collection, and storage of data that includes location and other information about passenger vehicles. As described in the *Notice of Proposed Rulemaking*, consumer acceptance of vehicle-to-vehicle technologies—which will depend on addressing consumer privacy concerns, among other concerns—is crucial to achieving the expected safety benefits of this technology. As a result, NHTSA expects manufacturers to take steps to minimize consumer privacy risks by providing a clear and transparent vehicle-to-vehicle privacy notice to consumers.

Similarly, in September 2016, NHTSA issued the *Federal Automated Vehicles Policy*,[72] to speed the delivery of an initial regulatory framework and best practices to guide manufacturers and other entities in the safe design, development, testing, and deployment of highly automated vehicles (e.g., vehicles systems capable of monitoring the driving environment). As described in this voluntary guidance, NHTSA views automated vehicle technology as capable of bringing significant safety benefits. The guidance, among other things, outlined a set of privacy principles and recommended that automakers manufacturing automated vehicle technologies adopt these or similar principles. In addition, manufacturers and other entities are asked to voluntarily provide

[71]NHTSA is proposing to issue a new Federal Motor Vehicle Safety Standard No. 150, to require all new light vehicles to be capable of vehicle-to-vehicle communications, such that they will send and receive Basic Safety Messages to and from other vehicles. *See* V2V Communications, 82 Fed. Reg. 3854 (proposed Jan. 12, 2017) (to be codified at 49 C.F.R. pt. 571). Dec. 2016. As of March 2017, DOT rulemakings are being evaluated in accordance with Executive Orders 13771 and 13777.

[72]See NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety (*September 2016). NHTSA requested comments on the *Federal Automated Vehicle Policy* from September to November 2016. According to NHTSA officials, as of April 2017, the *Federal Automated Vehicle Policy* is being reviewed internally.

information on how the guidance is being followed, including how they are addressing privacy.[73]

According to officials from FTC and NHTSA, in recent years the agencies have collaborated on vehicle data privacy and coordinated their respective efforts in this area. For example, recently, FTC and NHTSA staff has met monthly to discuss cybersecurity and privacy issues related to passenger vehicles. FTC and NHTSA also hosted a workshop in June 2017 on consumer privacy and security issues posed by automated and connected vehicles. Specifically, the workshop aimed to bring together multiple industry stakeholders, consumer advocates, academics, and government regulators to discuss various issues, including potential benefits and challenges posed by the collection of connected and automated vehicle data.

In addition to FTC and NHTSA, other federal agencies doing work on privacy issues include the National Institute of Standards and Technology and the National Telecommunications and Information Administration within the Department of Commerce. For example, in January 2017, the National Institute of Standards and Technology issued a report recommending practices for including privacy risk assessments when designing federal systems, and that according to agency officials, could also serve as guidance for private companies, including automakers.[74] In addition, the National Telecommunications and Information Administration has convened multistakeholder processes with industry and other stakeholders that focused on developing voluntary codes of conduct for the commercial use of emerging technologies, such as facial recognition technology. According to National Telecommunications and Information Administration officials, no additional privacy focused multistakeholder processes are planned at this time.

[73]As described in the policy, the Vehicle Performance Guidance, of which the request that manufacturers provide a safety assessment letter is a part, will not take effect until after NHTSA completes the process required by the Paperwork Reduction Act. Once that process is complete and NHTSA has published a notification in the Federal Register, the reporting provision in the Vehicle Performance Guidance outlined in the *Federal Automated Vehicles Policy* will be in effect.

[74]See, National Institute of Standards and Technology, *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems* (January 2017).

Selected Stakeholders Said NHTSA's Evolving Privacy Role is Unclear

The auto industry is currently undergoing a rapid evolution as vehicles become more connected and automated. For example, most automakers and industry associations in our review agreed that auto technology is rapidly evolving, and some of these stakeholders noted that the auto industry more broadly is evolving. As several of these stakeholders told us, this evolution will result in more data—including more sensitive data—being collected, used, and shared.

NHTSA's recent actions on emerging vehicle technologies align with the agency's safety mission, authority, and goals. However, NHTSA has not clearly defined and communicated its roles and responsibilities related to the privacy of connected vehicle data to stakeholders. Specifically, according to some automakers and all industry associations we spoke with, NHTSA's recent actions on emerging vehicle technologies have left stakeholders without a clear understanding of the agency's role with respect to privacy.[75] For example, three automakers noted that NHTSA appears to be more involved in data privacy as reflected by the *Federal Automated Vehicles Policy*. One automaker also questioned whether NHTSA was coordinating on data privacy issues with other relevant federal agencies. Five industry associations told us that NHTSA appears to have an interest in the area of privacy. Four of these associations also told us that NHTSA might have a role in monitoring its members' use of connected vehicle data, but the four were not sure. In addition, in public comments filed on the *Federal Automated Vehicles Policy*, one auto industry trade group questioned whether considering privacy issues is consistent with NHTSA's safety mission and suggested that certain privacy provisions in the policy exceeds NHTSA's current statutory authority. In contrast, all 11 automakers that discussed this topic and all industry associations in our review told us that FTC's role in this area is clear.[76] For example, representatives of both auto industry associations told us that they had chosen to notify the FTC about their members' implementation of the *Consumer Privacy Protection Principles* because FTC would be the federal agency to enforce and hold automakers

[75]Of the total 16 automakers in our review, 9 did not discuss NHTSA's privacy role. Three of the 7 automakers that did discuss this issue indicated that NHTSA's role related to privacy is unclear.

[76]Of the total 16 automakers in our review, 11 discussed FTC's role.

accountable to these principles. NHTSA officials acknowledged that some stakeholders may be uncertain whether and, if so, to what extent it has authority to address any privacy issues with respect to motor vehicles.

The *Standards for Internal Control in the Federal Government* call for agencies to identify, analyze, and respond to significant changes, and in response to such changes, to periodically reevaluate and further define key agency roles and responsibilities. These standards also direct agencies to clearly communicate relevant information—such as the agencies' roles, responsibilities, and important changes to these—to external parties. These standards are intended, among other things, to help agencies manage change associated with shifting environments and evolving demands and priorities.[77] We have also previously found that interagency collaboration is enhanced when agencies, among other things, ensure that their roles and responsibilities are clearly defined.[78] By agreeing on and clearly defining roles and responsibilities, agencies can clarify which agency will do what, organize their joint and individual efforts, and facilitate better decision making. As previously described, NHTSA and FTC have collaborated on the potential privacy risks posed by new vehicle technologies; clarifying NHTSA's role could therefore further enhance collaboration with FTC and other federal counterparts. Furthermore, if NHTSA more clearly defined its roles and responsibilities for protecting the privacy of connected vehicle data, industry stakeholders would have a better understanding of how the agency intends to oversee the privacy of data generated by emerging vehicle safety technologies and which agency is responsible for privacy as the connected vehicle landscape continues to evolve.

Conclusions

In recent years, connected vehicles have become more common, offering consumers a number of benefits but also increasing the potential for privacy risks. Currently, automakers are reportedly collecting, using, and sharing connected vehicle data on a fairly limited basis and are, at least

[77]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). These standards provide the overall framework for establishing and maintaining an effective internal control system for the federal government.

[78]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

partially, using leading privacy practices to protect that data. However, experts and others have raised a number of consumer privacy concerns, including whether such data—including sensitive information such as a driver's location and behavior—are being adequately protected. No single federal agency oversees data privacy issues. However, FTC has the primary role—one that is clearly defined and reinforced through its enforcement actions against companies that have engaged in unfair and deceptive practices, such as violating their own privacy practices or failing to implement reasonable security practices. Although NHTSA has a clear role in overseeing the safety of the estimated 265 million passenger vehicles on U.S. roads today, industry stakeholders are unclear about NHTSA's role with respect to vehicle data privacy, due to recent agency actions on automated vehicles and vehicle-to-vehicle technology.

With the anticipated increase in the number of connected vehicles on U.S. roads in the near future—and with it, the financial incentives for automakers and others to more widely collect, use, and share vehicle and driver data—it is important for NHTSA to define and communicate its privacy roles and responsibilities. If NHTSA makes its roles and responsibilities clearer, industry stakeholders will likely have a better understanding of its oversight role for emerging vehicle technologies, and NHTSA will likely be more effective in collaborating with FTC and other federal agencies. However, if that opportunity is missed, consumers may not fully embrace emerging technologies with potential safety benefits, such as vehicle-to-vehicle technology and automated vehicles. With a forward-looking approach to identify changes in the environment and clarifying its roles and responsibilities as needed in response, NHTSA can anticipate and—in collaboration with FTC—better plan for the anticipated changes that could impact the privacy of many Americans.

Recommendation for Executive Action

The Secretary of Transportation should direct NHTSA to

- define, document, and externally communicate the agency's roles and responsibilities in relation to connected vehicle data privacy.

Agency Comments

We provided a draft of this report to the Departments of Transportation (DOT), Commerce, and Justice, FTC, and the Federal Communications

Commission for review and comment. We received written comments from DOT, which are reprinted in appendix IV. We also received technical comments from DOT and FTC, which we have incorporated, as appropriate.

DOT concurred with our recommendation to define, document, and externally communicate the agency's roles and responsibilities in relation to connected vehicle data privacy. Among other things, DOT reiterated the importance of consumer privacy and how it considers the privacy implications of its regulations and voluntary guidance, such as in the proposed vehicle-to-vehicle rulemaking.

The Departments of Commerce and Justice and the Federal Communications Commission reviewed our report, but did not have any comments.

As agreed with your offices, 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 Secretaries of Transportation, Commerce, and Justice and the Chairs of the Federal Trade Commission and Federal Communication Commission, and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-2834 or wised@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 V.

David J. Wise
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

This report addresses the following objectives: (1) the types of data collected by connected vehicles and transmitted to automakers and how, if at all, selected automakers use and share these data, (2) the extent to which selected automakers' privacy policies for connected vehicles align with leading practices, (3) selected experts' views on privacy issues related to the commercial use of data collected by connected vehicles, and (4) federal roles and efforts related to the privacy of data collected by connected vehicles.

To address all of our objectives, we reviewed applicable federal statutes and regulations, our prior work,[1] and reports by other federal agencies, academics, and research organizations on privacy and connected technologies. We interviewed representatives of three organizations that advocate protecting the privacy of consumers' data identified and selected based on their contributions to our prior work.[2] We also interviewed eight industry associations representing automakers, automotive suppliers, application developers, and telecommunication companies. The industry associations we interviewed were: Association of Global Automakers, Alliance of Automobile Manufacturers, Application Developers Alliance, Connected Vehicle Trade Association, Consumer Technology Association, CTIA-The Wireless Association, Motor and Equipment Manufacturers Association, and the National Automobile Dealers Association.

To determine types of data collected from connected vehicles and how, if at all, these data are used, we conducted semi-structured interviews with representatives of 16 automakers and 3 other industry stakeholders. We attempted to interview most of the automakers selling passenger vehicles

[1] For example, see GAO, In-*Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers*, GAO-14-81 (Washington, D.C.: Dec. 6, 2013) and GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: March 24, 2016).

[2] For example, GAO-14-81 and GAO, *Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking,* GAO-16-317 (Washington, D.C.: Apr. 21, 2016).

in the United States and identified them using the membership lists of two automotive industry trade associations, the Alliance of Automobile Manufacturers and the Association of Global Automakers. We selected automakers to interview based on their 2015 U.S. market share, specifically, a market share that was larger than zero. Based on our discussions with the automotive trade associations, we excluded two automakers due to their very small U.S. market share, and two other automakers we contacted told us they no longer sell passenger vehicles in the U.S. We identified and selected one additional automaker, which is not a member of these automotive industry trade associations, due to its growing market share and high profile in the connected vehicle market. Of the 19 automakers we contacted, three did not respond to our interview request. For the complete list of automakers we interviewed, see table 3.

Table 3: Selected Automakers Interviewed and Their Vehicle Brands

Automakers	Relevant Vehicle Brands
BMW	BMW, Rolls Royce, Mini
Fiat Chrysler Automobiles	Chrysler, Dodge, Fiat, Jeep, Ram
Ford Motor Company	Ford and Lincoln
General Motors	Buick, Cadillac, Chevrolet, GMC
Honda Motor Company	Acura and Honda
Hyundai Motor America	Hyundai and Genesis
Kia Motors Corporation	Kia
Maserati North America	Maserati
Mazda USA	Mazda
Mercedes-Benz USA LLC	Mercedes-Benz
Mitsubishi Motors Corporation	Mitsubishi
Subaru of America, Inc.	Subaru
Tesla Motors, Inc.	Tesla
Toyota Motor Corporation	Lexus and Toyota
Volkswagen Group	Audi, Porsche, Volkswagen
Volvo Cars	Volvo

Source: GAO. | GAO-17-656

We identified and selected other industry stakeholders based on their industry roles, specifically their roles as telecommunication companies,

telematics service providers, and application developers.[3] Of the 12 other industry stakeholders we contacted, we interviewed three stakeholders representing two telecommunications companies and one telematics service provider. Given the small number of other industry stakeholders interviewed, the names of these companies are not included in this report. We used a semi-structured format in our interviews with automakers and other industry stakeholders and asked each type of stakeholder the same set of questions. For example, we asked each automaker what types of data it collects, how these data are used, and how they share these data. We asked each of the 13 automakers that offer connected vehicles a set of additional questions to clarify its use and sharing of data and its privacy practices. After interviewing selected automakers, we summarized and analyzed their responses to identify themes relevant to our research objectives, such as the types of data collected. The views and information gathered through our interviews with selected automakers and industry stakeholders cannot be generalized to the industry as a whole. However, the 16 selected automakers we interviewed produce over 25 vehicle brands and represented around 90 percent of the U.S. passenger vehicle sales market share in 2015.

To determine the extent to which selected automakers' reported privacy practices and written privacy notices (collectively we refer to these as "privacy policies") for connected vehicles reflect leading practices, we identified leading practices related to privacy using several widely recognized sources. The privacy frameworks and reports we used for this analysis are: (1) the Organisation for Economic Co-operation and Development's *The OECD Privacy Framework* (known as the "*Fair Information Practice Principles"* (FIPPs); (2) the Federal Trade Commission's (FTC) report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012); (3) FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (2015); (4) the National Highway and Transportation Administration's (NHTSA) *Federal Automated Vehicles Policy* (2016); and (5) the National Institute of Standards and Technology's *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems* (2017). We compared the leading practices identified in each source and grouped practices into similar categories. We did not deem any practices from the sources to be irrelevant for our review on

[3]Telematics service providers may offer services directly to vehicle drivers for a subscription or through a contract with automakers. These services typically include safety, security, or convenience features to drivers.

connected vehicles, but we did determine that similar identified practices could be combined into one leading practice. The privacy leading practices we used for our analysis are transparency, focused data use, data security, data accuracy and access, individual control, and accountability. To determine the extent to which automakers' privacy policies reflect these leading practices, we analyzed selected automakers' written privacy notices through a document review and reported privacy practices related to connected vehicles based on automakers' responses to semi-structured interview questions. Of the 16 automakers we interviewed, 13 offered connected vehicles at the time we spoke to them. While many of these automakers offer several brands, one automaker had different written privacy notices for its three vehicle brands sold in the U.S. As such, we analyzed a total of 15 sets of privacy policies (their written notices and reported privacy practices).

To analyze the written privacy notices, we developed questions to determine whether an automaker's written privacy notice specifically addressed the various elements of a privacy leading practice.[4] We conducted a test case with one automaker's written privacy notice and made needed revisions to the questions. Then, one analyst coded each of the 15 written privacy notices using NVivo software.[5] A second analyst reviewed the coding and confirmed the accuracy of the results.[6]

To analyze the reported privacy practices, we conducted a content analysis of automakers' interview responses to questions related to their privacy practices. All automakers were asked the same set of questions, and we conducted follow-up with each automaker offering connected vehicles to ensure consistency in responses and ensure that we asked

[4]In assessing the transparency of the written privacy notices, readability was judged using *Flesch Reading Ease* scores. Scores fall on a scale from 0 to 100, with 0 being nearly impossible to read and 100 being simple enough for a fifth grader to read. A score of 60 or above qualifies as "plain language." The formula is based on average sentence length and average word length. The version we used was included in the Microsoft Word processing software. As GAO has previously reported, the *Flesch Reading Ease* score is one of the most widely used, tested, and reliable formulas for calculating readability. See GAO-16-750, *Equal Employment Opportunity: Strengthening Oversight Could Improve Federal Contractor Nondiscrimination Compliance* (Washington, D.C.: September 2016).

[5]The written notices in the analysis were provided to us by the automakers, and were those in effect as of January 1, 2017. Some automakers identified more than one written notice as relevant.

[6]For a full list of the questions used to analyze automakers' privacy policies, see appendix III.

questions related to each of the leading privacy practices identified as relevant for connected vehicles for the purposes of this report. As part of our follow up work, we asked selected automakers questions directly related to the leading privacy practices. One analyst coded the interview responses and a second analyst reviewed and confirmed the accuracy of the coding.

To assess whether an automaker's policies reflected each of these leading privacy practices, we used the following scale:

- *Substantially reflected*: a company met most (70 percent or more) of the elements of this leading practice.
- *Partially reflected*: a company met about half of the elements of this leading practice.
- *Minimally reflected*: a company met less than half of the elements of this leading practice.

For each of the six leading practices, there were between 5 to 10 questions of equal weight that we used to determine the extent to which a practice was reflected.

As noted above, our analysis of automakers' privacy policies is based on written notices and reported practices obtained through interviews. We did not conduct a compliance review, as the leading practices used in this report are not legally binding. We also did not evaluate the extent to which selected automakers follow their reported privacy policies.

To determine selected experts' views on privacy issues related to the commercial use of data collected by connected vehicles, we interviewed 16 subject matter experts in connected vehicles or privacy. We identified a prospective pool of subject matter experts through reviewing our prior reports, related National Academy of Sciences panels, relevant literature, and recommendations from other interviewees. We selected subject matter experts using eight criteria: relevant background, selected academic publications and technical reports, selected presentations at conferences, selected popular source articles, selected testimonies, selected instances of interviews on prior engagements, selected professional service and appointments, and recommendations from other interviewees. Those organizations and individuals that had relevant experience in at least four of our eight criteria were deemed experts for the purposes of our review (see table 4 for the full list of experts we interviewed).

Table 4: Selected Subject Matter Experts Interviewed

Center for Automotive Research (CAR)
Center for Democracy and Technology (CDT)
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)
Future of Privacy Forum (FPF)
World Privacy Forum (WPF)
Kendall Burman, Cybersecurity and Data Privacy Counsel, Mayer Brown
Frank Douma, Research Scholar at the Center for Transportation Studies, University of Minnesota
Dorothy Glancy, Professor of Law, Santa Clara University School of Law
Aleecia McDonald, Privacy Researcher and Non-Resident Fellow at the Center for Internet & Society, Stanford University
Lee Rainie, Director of Internet, Science, and Technology, Pew Research Center
Catherine Tucker, Sloan Distinguished Professor of Management, Massachusetts Institute of Technology
Bryant Walker Smith, Assistant Professor of Law, University of South Carolina
Andre Weimerskirch, Vice President, Cyber Security at LEAR Corporation
William Whyte, Chief Scientist, Security Innovation
Johanna Zmud, Senior Research Scientist, Texas A&M Transportation Institute

Source: GAO. | GAO-17-656

As part of these semi-structured interviews, we presented each selected expert with general privacy concerns about the commercial use of data we identified from our prior reports,[7] FTC reports, and preliminary interviews with organizations that advocate protecting consumers' data privacy. We asked each selected expert to what extent these privacy concerns were relevant to data collected through connected vehicles. After interviewing selected experts, we summarized and analyzed their responses to identify themes relevant to our research objective. The views and information gathered through our interviews with subject matter experts cannot be generalized to all such experts, but they do provide insight into relevant privacy concerns and solutions.

To examine federal roles and efforts related to the privacy of data collected from connected vehicles, we reviewed relevant documents and interviewed officials from four federal agencies—FTC, Department of

[7]For example, see GAO, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015).

Transportation, Department of Commerce, and Federal Communications Commission[8]—that we identified as having privacy and consumer protection responsibilities potentially related to connected vehicles. We also discussed with selected experts, automakers, other industry stakeholders, and industry associations the federal laws that may apply in this context and related federal efforts and roles. Because of DOT's role in overseeing motor vehicles, we compared DOT's efforts to reevaluate and define key agency roles and responsibilities as new vehicle technologies emerge with pertinent *Standards for Internal Control in the Federal Government*[9] and practices identified in our prior work on agency collaboration.[10]

We conducted this performance audit from April 2016 to July 2017 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.

[8]We spoke with Federal Communications Commission officials regarding their *Order on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (released Nov. 2, 2016) to understand the relevance, if any, this order may have to connected vehicles as discussed in our review. FCC officials said that this order would not apply to automakers, but could apply to telecommunication carriers providing internet connectivity through vehicles, if certain parameters were satisfied. However, pursuant to authority provided by the Congressional Review Act, the President signed a joint resolution providing for congressional disapproval of the rule. We also met with officials from the Department of Justice to understand its role regarding connected vehicle data; however, given our focus on commercial uses of connected vehicle data, we did not conduct additional audit work related to their role or activities.

[9]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). These standards provide the overall framework for establishing and maintaining an effective internal control system for the federal government.

[10]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

Appendix II: Summary of Relevant Privacy Frameworks and Self-Regulatory Principles

Table 5: Summary of the Organisation for Economic Co-operation and Development's (OECD) Fair Information Practice Principles (FIPPs)

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. | GAO-17-656

Note: This table summarizes the "Basic Principles" of the 2013 OECD Privacy Framework, and they are commonly referred to as the OECD's *Fair information Practice Principles* (FIPPs). The 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. In 1980, the OECD developed a revised version that was widely adopted. In 2013, the OECD published its first revision since its original version of the Privacy Framework.

Table 6: Summary of the *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*

Principle	Description
Transparency	Provide consumers with access to clear, meaningful notices about the collection, use, and sharing of certain vehicle information ("covered information").[a]
Choice	Offer consumer some choice regarding the collection, use, and sharing of vehicle information.
Respect for context	Use and share vehicle information consistent with the context in which it was collected and considering the likely impact on consumers.
Data minimization, de-identification, and retention	Collect vehicle information and retain this information only as needed for legitimate business purposes.
Data security	Implement reasonable measures to protect vehicle information against loss and unauthorized access or use.
Integrity and access	Implement reasonable measures to maintain the accuracy of vehicle information and commit to give consumers the means to review and correct personal subscription information (e.g., name, address, and payment information).
Accountability	Take reasonable steps to ensure that they and other entities that receive vehicle information follow the *Consumer Privacy Protection Principles*.

Source: Alliance of Automobile Manufacturers and Association of Global Automakers. | GAO-17-656

Note: Like other industries, the automobile industry developed a set of privacy principles— the *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services ("Consumer Privacy Protection Principles")*. These principles are a self-regulatory framework influenced by the OECD's *Fair information Practice Principles* (FIPPs) and were adopted by most automakers with vehicle sales in the U.S. The *Consumer Privacy Protection Principles*, which went into effect January 2, 2016, ask participating companies to commit to these principles.

[a]The *Consumer Privacy Protection Principles* outline the vehicle information, "covered information," eligible for these protections, including personal subscription information: information provided by individuals during the subscription or registration process, such as name, address, credit card number or email address; biometrics: information about a consumer's physical or biological characteristics that serves to identify the person; driver behavior information: information about how a person drives a vehicle, such as vehicle speed or seat belt use; and geolocation information: the precise geographic location of a vehicle.

Appendix III: Analysis of Automakers' Reported Privacy Policies and Results

We assessed the extent to which selected automakers' reported policies reflected each of the leading privacy practices we identified. We included in this analysis those 13 automakers offering connected vehicle services. However, one of these 13 automakers has different written privacy notices and reported privacy practices for its three affiliated brands. As a result, our analysis of automakers' privacy policies included 15 sets of privacy policies. We reviewed the automakers' written privacy notices and responses to specific interview questions focused on their use of these practices. We also asked automakers to confirm their answers to the interview questions directly related to the leading privacy practices. We used the following scale to categorize the extent to which each automaker's policies reflected each leading practice:[1]

- *Substantially reflected:* automaker met most (70 percent or more) of the elements of this leading practice.
- *Partially reflected:* automaker met about half (50 to 69 percent) of the elements of this leading practice.
- *Minimally reflected:* automaker met less than half or none of the elements of this leading practice.

For this assessment, we used a total of 43 questions, each of which was given equal weight, across the six identified leading practices:

1) transparency,

2) focused data use,

3) data security,

4) data access and accuracy,

[1]This was not a compliance review of automakers. As leading practices, these are not legally binding. We did not evaluate whether the automakers actually follow their reported policies.

5) individual control, and

6) accountability.

Some assessment questions relate to automakers' written privacy notices and others relate to interview questions we asked about the automaker's use of the leading practices. The 6 tables below include, for each leading practice: the assessment questions, the results for each automaker, and an overall summary of how fully all the selected automakers' policies reflected the practice.

Table 7: Leading Practice Assessment: *Transparency (*1) for Automakers A through O

	Question	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Does / is the written notice:	Yes. Outline types of personal data collected?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2. Describe how personal data will be collected?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	3. Include the purpose(s) for which personal data will be collected?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4. Include inclusive list of types of personal data collected?	No	No	No	No	No	No	No	Yes	No	No	No	No	No	No	No
	5. Include inclusive list of the purposes for which the automaker will use the personal data?	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes
	6. Outline whether and when personal data may be shared with third parties?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	7. Written in plain language?[a]	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
	8. Divided into sections such as data collected?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
As reported in interviews:	9. Does the automaker have a privacy policy that applies to technologies and services pre-installed in vehicles that is publicly available?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Totals—Assessment	**"Yes" answers (out of 9)**	**6**	**6**	**6**	**6**	**7**	**6**	**6**	**7**	**6**	**6**	**6**	**6**	**6**	**6**	**7**
	Category: (Substantially, Partially, or Minimally Reflected)	Partial	Partial	Partial	Partial	Subst.	Partial	Partial	Subst.	Partial	Partial	Partial	Partial	Partial	Partial	Subst.
	Overall Assessment Summary:	**Most automakers' reported privacy policies (Yes2 out of Yes5) partially reflected this leading practice.**														

Source: GAO analysis of automakers' privacy notices and interviews | GAO-17-656

[a]Readability was judged using Flesch Reading Ease scores. Scores fall on a scale from 0 to 100, with 0 being nearly impossible to read and 100 being simple enough for a fifth grader to read. A score of 60 or above qualifies as "plain language." The formula is based on average sentence length and average word length. The version we used was included in the Microsoft Word software.

Table 8: Leading Practice Assessment: *Focused Data Use* (2) for Automakers A through O

	Question	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Does the written notice:	Yes. Include a section about how collection and use of data will be limited?	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes
	2. State personal data will not be used for purpose(s) besides specified in policy?	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
	3. Clarify whether personal data will be de-identified?	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4. Describe how personal data will be de-identified?	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
	5. State whether de-identified or anonymized data may be shared with 3rd parties?	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
	6. Include length of time automaker will retain personal data?	No	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No
As reported in interviews:	7. Does the automaker use policy solutions to protect data privacy: limiting data collection?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	8. Does the automaker use policy solutions to protect data privacy: limiting data retention?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	9. Does the automaker use technological solutions: using de-identified or anonymized data?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	YesNo. Does the automaker use technological solutions: using aggregated data?	Yes	Yes	Yes	Yes	Yes	No	Not answered	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	Question	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Total Assessment	**Number of "Yes" answers (out of YesNo)**	**7**	**7**	**7**	**6**	**6**	**4**	**6 (out of 9)[a]**	**7**	**6**	**6**	**7**	**7**	**6**	**7**	**6**
	Category: (Substantially, Partially, or Minimally Reflected)	Subst.	Subst.	Subst.	Partial	Partial	Min.		Subst.	Partial	Partial	Subst.	Subst.	Partial	Subst.	Partial
	Overall Assessment	**Almost half of automakers' reported privacy policies (7 out of Yes5) substantially reflected this leading practice, and 6 partially reflected the practice.**														

Source: GAO analysis of automakers' privacy notices and interviews | GAO-Yes7-656

[a]Some interview questions were not answered by all automakers. In those cases, the total number of "yes" answers possible was decreased. Also, for such cases, a category was not assigned to the automaker for the leading practice.

Table 9: Leading Practice Assessment: *Data Security* (3) for Automakers A through O

	Question	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Does the written notice:	Yes. Include a section addressing how personal data will be safeguarded?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2. Explain for consumers the safeguards taken to ensure data are secure?[a]	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	3. Provide at least one example of industry standard practices used?	Yes	No	No	Yes	No	Yes	No	Yes	Yes	No	No	No	Yes	No	Yes
As reported in interviews:	4. Does the automaker use technological solutions to safeguard data from unauthorized access or use, such as using firewalls, etc.?[a]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	5. Does the automaker participate in the Auto-Information Sharing and Analysis center (Auto-ISAC)?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
	6. Does the automaker conduct privacy risk assessments?	Yes	Yes	Yes	Yes	Yes	No	Not answered	Yes	Not answered	Yes	Yes	Yes	Yes	Not answered	Yes
Totals—Assessment	**Number of "Yes" answers (out of 6)**	**6**	**5**	**5**	**6**	**5**	**5**	**2 (out of 5)[b]**	**6**	**5 (out of 5)[b]**	**5**	**5**	**5**	**6**	**3 (out of 5)[b]**	**6**
	Category: (Substantially, Partially, or Minimally Reflected)	Subst.	Subst.	Subst.	Subst.	Subst.	Subst.		Subst.		Subst.	Subst.	Subst.	Subst.		Subst.
	Overall Assessment	**The majority of automakers' reported privacy policies (Yes2 out of Yes5) substantially reflected this leading practice.** **The remaining automakers did not answer all the assessment questions.**														

Source: GAO analysis of automakers' privacy notices and interviews | GAO-Yes7-656

[a]Although related, these two questions are not the same. The first relates to whether the written notice explains safeguards used, and the second is about whether the automaker actually uses safeguards.

[b]Some interview questions were not answered by all automakers. In those cases, the total number of "yes" answers possible was decreased. Also, for such cases, a category was not assigned to the automaker for the leading practice.

Table YesNo: Leading Practice Assessment: *Data Accuracy and Access* (4) for Automakers A through O

	Question	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Does the written notice:	Yes. Include a section addressing data accuracy and access?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes
	2. Outline for consumers measures automaker takes to ensure personal data are accurate?[a]	No	Yes	No	No	No	No	No	Yes	No	No	No	No	No	Yes	Yes
	3. Include how consumers can access own personal data?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes
	4. Include how consumers can correct or challenge data?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes
As reported in interviews:	5. Can consumers access and / or correct their own data collected from connected vehicles?	Not answered	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not answered	Yes	Yes	Not answered	Yes	Not answered	Yes
	6. Does the automaker take steps to ensure that data collected from connected vehicles are accurate?[a]	Not answered	Yes	Yes	Yes	Yes	Not answered	Yes	Yes	Not answered	Yes	Yes	Not answered	Yes	Not answered	Yes
Totals—Assessment	**Number of "Yes" answers (out of 6)**	**3 (out of 4)[b]**	**6**	**5**	**5**	**5**	**4 (out of 5)[b]**	**2**	**6**	**3 (out of 4)[b]**	**2**	**2**	**4 (out of 4)[b]**	**5**	**4 (out of 4)[b]**	**6**
	Category: (Substantially, Partially, or Minimally Reflected)		Subst.	Subst.	Subst.	Subst.		Min.	Subst.		Min.	Min.		Subst.		Subst.

	Overall Assessment	**Almost half of automakers' reported privacy policies (7 out of Yes5) substantially reflected this leading practice.** **Three policies minimally reflected the practice, and 5 automakers did not answer all assessment questions.**

Legend: Yes = yes, No = no, — = not answered

Source: GAO analysis of automakers' privacy notices and interviews | GAO-Yes7-656

[a]Although related, these two questions are not the same. The first relates to whether the written notice explains measures used to consumers, and the second is about whether the automaker actually uses such measures to ensure data accuracy.

[b]Some interview questions were not answered by all automakers. In those cases, the total number of "yes" answers possible was decreased. Also, for such cases, a category was not assigned to the automaker for the leading practice.

Table YesYes: Leading Practice Assessment: *Individual Control* (5) for Automakers A through O

	Question	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Does the written notice:	Yes. Include a section addressing consumer's right to control over personal data?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2. Describe how consumer may choose to not allow collection of some data types?	No	No	No	No	No	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes
	3. Indicate how consumer can opt in to having all personal data collected to use a certain service?	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	4. Indicate how consumers can withdraw permission to transmit data from vehicle?	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
As reported in interviews:	5. Does the automaker obtain explicit consent before extracting connected vehicle data?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	Question	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	6. Does the automaker obtain consent again after initiating the extracting of data (when the telematics service is renewed, at periodic intervals, etc.)?	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
	7. Is it possible for consumers to modify the type or quantity of data collected (without opting out of the service entirely)?	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Totals—Assessment	**Number of "Yes" answers (out of 7)**	**4**	**5**	**5**	**4**	**3**	**6**	**4**	**2**	**5**	**5**	**6**	**5**	**6**	**5**	**5**
	Category: (Substantially, Partially, or Minimally Reflected)	Partial	Subst.	Subst.	Partial	Min.	Subst.	Partial	Min.	Subst.	Subst.	Subst.	Subst.	Subst.	Subst.	Subst.
	Overall Assessment	**The majority of automakers' reported privacy policies (YesNo out of Yes5) substantially reflected this leading practice.** **The remainder of policies either partially (3) or minimally (2) reflected the practice.**														

Legend: Yes = yes, No = no

Source: GAO analysis of automakers' privacy notices and interviews | GAO-Yes7-656

Table Yes2: Leading Practice Assessment: *Accountability* (6) for Automakers A through O

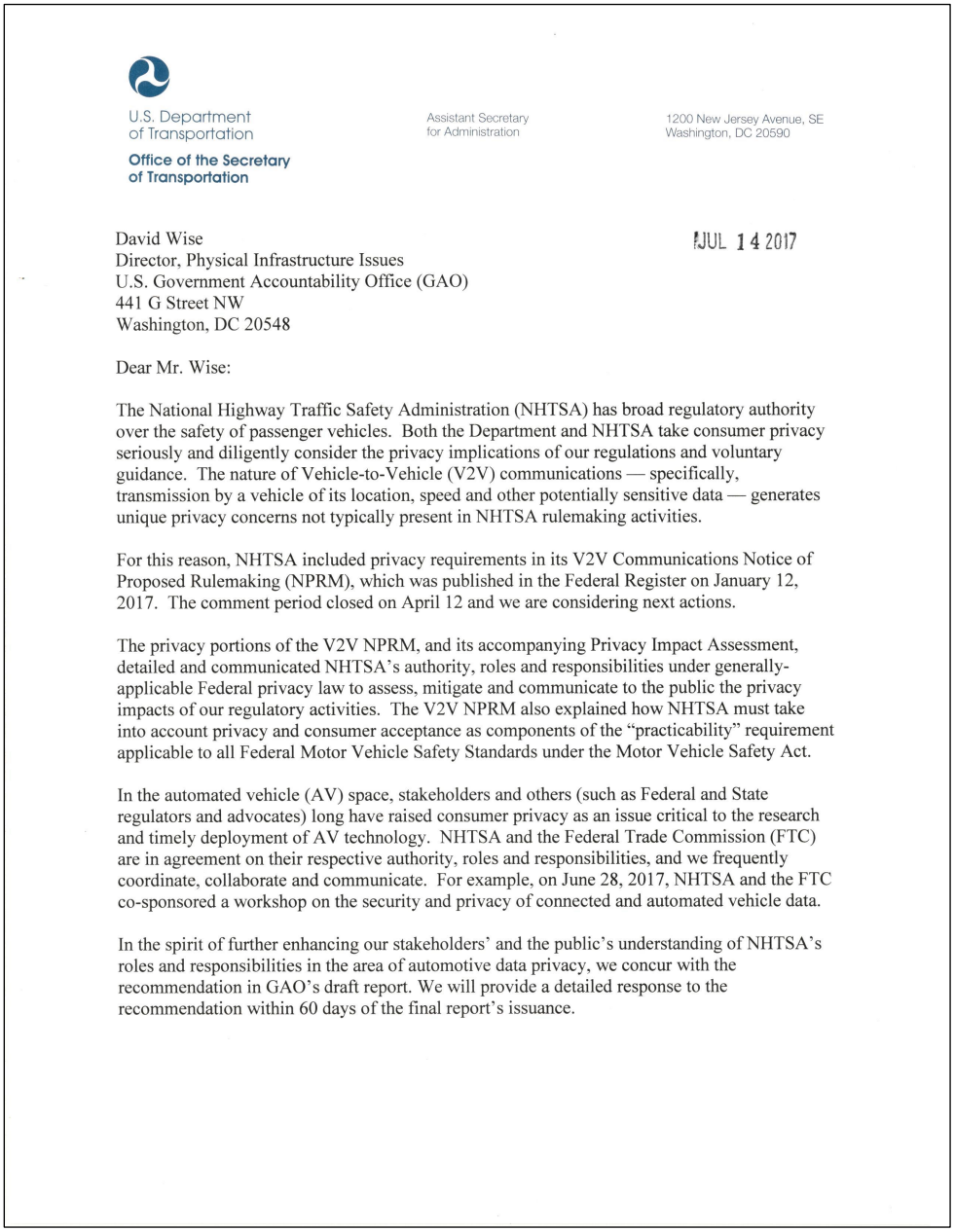
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Does the written notice:	Yes. Include a section addressing accountability for ensuring personal data are handled appropriately?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	2. Provide point of contact of entity responsible for protecting data?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	3. Outline obligations affiliated third parties must meet to receive personal data?	Yes	No	No	Yes	Yes	No	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes
As reported in interviews:	4. Does the automaker require that the staff who handle connected vehicle data meet certain requirements, such as required training?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes	Yes	Yes	—	Yes
	5. Does the automaker require that affiliated third parties (e.g., third-party service providers) that receive data collected from connected vehicles meet certain data security and privacy requirements?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes
Totals—Assessment	**Number of "Yes" answers (out of 5)**	**5**	**4**	**4**	**5**	**5**	**4**	**3**	**5**	**3 (out of 4)[a]**	**4**	**5**	**5**	**5**	**2 (out of 3)[a]**	**5**
	Category: (Substantially, Partially, or Minimally Reflected)	Subst.	Subst.	Subst.	Subst.	Subst.	Subst.	Partial	Subst.		Subst.	Subst.	Subst.	Subst.		Subst.
	Overall Assessment	**Most automakers' reported privacy policies (Yes2 out of Yes5) substantially reflected this leading practice. Two of the remaining automakers did not answer all assessment questions.**														

Legend: Yes = yes, No = no, — = not answered

Source: GAO analysis of automakers' privacy notices and interviews. | GAO-Yes7-656

[a]Some interview questions were not answered by all automakers. In those cases, the total number of "yes" answers possible was decreased. Also, for such cases, a category was not assigned to the automaker for the leading practice.

Appendix IV: Comments from the Department of Transportation



U.S. Department of Transportation
Office of the Secretary of Transportation

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

JUL 14 2017

David Wise
Director, Physical Infrastructure Issues
U.S. Government Accountability Office (GAO)
441 G Street NW
Washington, DC 20548

Dear Mr. Wise:

The National Highway Traffic Safety Administration (NHTSA) has broad regulatory authority over the safety of passenger vehicles. Both the Department and NHTSA take consumer privacy seriously and diligently consider the privacy implications of our regulations and voluntary guidance. The nature of Vehicle-to-Vehicle (V2V) communications — specifically, transmission by a vehicle of its location, speed and other potentially sensitive data — generates unique privacy concerns not typically present in NHTSA rulemaking activities.

For this reason, NHTSA included privacy requirements in its V2V Communications Notice of Proposed Rulemaking (NPRM), which was published in the Federal Register on January 12, 2017. The comment period closed on April 12 and we are considering next actions.

The privacy portions of the V2V NPRM, and its accompanying Privacy Impact Assessment, detailed and communicated NHTSA's authority, roles and responsibilities under generally-applicable Federal privacy law to assess, mitigate and communicate to the public the privacy impacts of our regulatory activities. The V2V NPRM also explained how NHTSA must take into account privacy and consumer acceptance as components of the "practicability" requirement applicable to all Federal Motor Vehicle Safety Standards under the Motor Vehicle Safety Act.

In the automated vehicle (AV) space, stakeholders and others (such as Federal and State regulators and advocates) long have raised consumer privacy as an issue critical to the research and timely deployment of AV technology. NHTSA and the Federal Trade Commission (FTC) are in agreement on their respective authority, roles and responsibilities, and we frequently coordinate, collaborate and communicate. For example, on June 28, 2017, NHTSA and the FTC co-sponsored a workshop on the security and privacy of connected and automated vehicle data.

In the spirit of further enhancing our stakeholders' and the public's understanding of NHTSA's roles and responsibilities in the area of automotive data privacy, we concur with the recommendation in GAO's draft report. We will provide a detailed response to the recommendation within 60 days of the final report's issuance.

We appreciate the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich, Director, Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if you would like to obtain additional details.

Sincerely,

Bryan Slater
Assistant Secretary for Administration

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

David Wise, 202-512-2834 or WiseD@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following individuals made important contributions to this report: Nancy Lueke (Assistant Director); Sarah Arnett (Analyst-in-Charge); Jessica Bryant-Bertail; Camilo Flores; Pamela Davidson; Delwen Jones; Josh Ormond; Eleni Orphanides; and John Villecco.

Appendix VI: Accessible Data

Data Table

Data Table for Figure 3: Selected Automakers' Reported Model Year 2017 Offerings of Connected Vehicles

Automaker	% of Model Year 2017 Vehicles offered with Connected Capabilities
A	100
B	100
C	100
D	100
E	85
F	70
G	60
H	50
I	43
J	35
K	3
L	0

Automaker	% of Model Year 2017 Vehicles offered with Connected Capabilities
M	0
N	0
O	0

Agency Comment Letter

Text of Appendix IV: Comments from the Department of Transportation

Page 1

David Wise

Director, Physical Infrastructure Issues

U.S. Government Accountability Office (GAO) 441 G Street NW

Washington , DC 20548

Dear Mr. Wise:

The National Highway Traffic Safety Administration (NHTSA) has broad regulatory authority over the safety of passenger vehicles. Both the Department and NHTSA take consumer privacy seriously and diligently consider the privacy implications of our regulations and voluntary guidance. The nature of Vehicle-to-Vehicle (V2V) communications - specifically, transmission by a vehicle of its location, speed and other potentially sensitive data -generates unique privacy concerns not typically present in NHTSA rulemaking activities.

For this reason, NHTSA included privacy requirements in its V2V Communications Notice of Proposed Rulemaking (NPRM), which was published in the Federal Register on January 12, 2017. The comment period closed on April 12 and we are considering next actions.

The privacy portions of the V2V NPRM , and its accompanying Privacy Impact Assessment , detailed and communicated NHTSA 's authority, roles and responsibilities under generally- applicable Federal privacy law

to assess, mitigate and communicate to the public the privacy impacts of our regulatory activities. The V2V NPRM also explained how NHTSA must take into account privacy and consumer acceptance as components of the "practicability" requirement applicable to all Federal Motor Vehicle Safety Standards under the Motor Vehicle Safety Act.

In the automated vehicle (AV) space, stakeholders and others (such as Federal and State regulators and advocates) long have raised consumer privacy as an issue critical to the research and timely deployment of AV technology. NHTSA and the Federal Trade Commission (FTC) are in agreement on their respective authority, roles and responsibilities, and we frequently coordinate, collaborate and communicate. For example, on June 28, 2017, NHTSA and the FTC co-sponsored a workshop on the security and privacy of connected and automated vehicle data.

In the spirit of further enhancing our stakeholders ' and the public's understanding of NHTSA 's roles and responsibilities in the area of automotive data privacy, we concur with the recommendation in GAO's draft report. We will provide a detailed response to the recommendation within 60 days of the final report 's issuance.

Page 2

We appreciate the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich , Director, Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if you would like to obtain additional details.

Bryan Slater

Assistant Secretary for Administration

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, LinkedIn, 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 and read The Watchblog.

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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548