Tracking & Hacking:

Security & Privacy Gaps Put American Drivers at Risk

ED MARKEY
United States Senator *for* Massachusetts

February 2015
www.markey.senate.gov

A report written by the staff of Senator Edward J. Markey (D-Massachussetts)

EXECUTIVE SUMMARY

New technologies in cars have enabled valuable features that have the potential to improve driver safety and vehicle performance. Along with these benefits, vehicles are becoming more connected through electronic systems like navigation, infotainment, and safety monitoring tools.

The proliferation of these technologies raises concerns about the ability of hackers to gain access and control to the essential functions and features of those cars and for others to utilize information on drivers' habits for commercial purposes without the drivers' knowledge or consent.

To ensure that these new technologies are not endangering or encroaching on the privacy of Americans on the road, Senator Edward J. Markey (D-Mass.) sent letters to the major automobile manufacturers to learn how prevalent these technologies are, what is being done to secure them against hacking attacks, and how personal driving information is managed.[1]

This report discusses the responses to this letter from 16 major automobile manufacturers: BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen (with Audi), and Volvo. Letters were also sent to Aston Martin, Lamborghini, and Tesla, but those manufacturers did not respond.

The responses reveal the security and privacy practices of these companies and discuss the wide range of technology integration in new vehicles, data collection and management practices, and security measures to protect against malicious use of these technologies and data. The key findings from these responses are:

1. Nearly 100% of cars on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions.
2. Most automobile manufacturers were unaware of or unable to report on past hacking incidents.
3. Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across all automobile manufacturers, and many manufacturers did not seem to understand the questions posed by Senator Markey.
4. Only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time, and most say they rely on technologies that cannot be used for this purpose at all.
5. Automobile manufacturers collect large amounts of data on driving history and vehicle performance.
6. A majority of automakers offer technologies that collect and wirelessly transmit driving history data to data centers, including third-party data centers, and most do not describe effective means to secure the data.
7. Manufacturers use personal vehicle data in various ways, often vaguely to "improve the customer experience" and usually involving third parties, and retention policies – how long they store information about drivers – vary considerably among manufacturers.
8. Customers are often not explicitly made aware of data collection and, when they are, they often cannot opt out without disabling valuable features, such as navigation.

These findings reveal that there is a clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle or against those who may wish to collect and use personal driver information.

In response to the privacy concerns raised by Senator Markey and others, the two major coalitions of automobile manufacturers recently issued a voluntary set of privacy principles by which their members have agreed to abide. These principles send a meaningful message that automobile manufacturers are committed to protecting consumer privacy by ensuring transparency and choice, responsible use and security of data, and accountability. However, the impact of these principles depend in part on how the manufacturers interpret them, because (1) the specific ways that transparency

1. http://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy

will be achieved are unclear and may not be noticed by the consumer, e.g., text in the user manual, (2) the provisions regarding choice for the consumer only address data sharing and do not refer to data collection in the first place, and (3) the guidelines for data use, security, and accountability largely leave these matters to the discretion of the manufacturers.

The alarmingly inconsistent and incomplete state of industry security and privacy practices, along with the voluntary principles put forward by industry, raises a need for the National Highway Traffic Safety Administration (NHTSA), in consultation with the Federal Trade Commission (FTC) on privacy issues, to promulgate new standards that will protect the data, security and privacy of drivers in the modern age of increasingly connected vehicles. Such standards should:

- Ensure that vehicles with wireless access points and data-collecting features are protected against hacking events and security breaches;
- Validate security systems using penetration testing;
- Include measures to respond real-time to hacking events;
- Require that drivers are made explicitly aware of data collection, transmission, and use;
- Ensure that drivers are given the option to opt out of data collection and transfer of driver information to off-board storage;

Require removal of personally identifiable information prior to transmission, when possible and upon consumer request.

INTRODUCTION AND METHODOLOGY

Today's cars and light trucks contain more than 50 separate electronic control units (ECUs), connected through a controller area network (CAN) or other network (such as Local Interconnect Networks or Flexray). Vehicle functionality, safety, and privacy all depend on the functions of these small computers, as well as their ability to communicate with one another. They also have the ability to record vehicle data to analyze and improve performance. On-board navigation technologies as well as the ability to integrate mobile devices with vehicle-based technologies have also fundamentally altered the manner in which drivers and the vehicles themselves can communicate during the vehicles' operation.

This new technology has also resulted in an increased ability to gather driving information. Such information-gathering abilities can be used by automobile manufacturers to provide customized service and improve customer experiences, but in the wrong hands such information could also be used maliciously. In particular, wireless technologies create vulnerabilities to hacking attacks that could be used to invade a user's privacy or modify the operation of a vehicle. Two recent developments highlight potential threats to both automobile security and to consumer privacy.

In a 2013 study that was funded by the Defense Advanced Research Projects Agency (DARPA), two researchers demonstrated their ability to connect a laptop to two different vehicles' computer systems using a cable, send commands to different ECUs through the CAN, and thereby control the engine, brakes, steering and other critical vehicle components.[2] In their initial tests with a laptop and two MY2010 vehicles from different manufacturers, they were able to cause cars to suddenly accelerate, turn, kill the brakes, activate the horn, control the headlights, and modify the speedometer and gas gauge readings.[3] More recently in 2014, those same researchers looked into the hackability of 21 different vehicle models from 10 different manufacturers, pointing out different levels of security in each vehicle with respect to wireless entry points, control points, and the types of computers than could be compromised.[4]

Before the researchers went public with their 2013 findings, they shared the results with the manufacturers in the hopes that the companies would address the identified vulnerabilities. But in response to the public release of the study, both companies reportedly noted that the researchers directly, rather than wirelessly, accessed the vehicles' computer systems, and referred to the need to prevent remote hacking from a wireless device. What the companies failed to note is that the DARPA study built on prior research that demonstrated that one could remotely and wirelessly access a vehicle's CAN bus through Bluetooth connections, OnStar systems, malware in a synced Android smartphone, or a malicious file on a CD in the stereo.[5]

A second, related area of concern relates to the increasing use of navigation or other technologies that could be used to record the location or driving history of those using them. A number of new services have emerged that permit the collection of a wide range of user data, providing valuable information not just to improve vehicle performance, but also potentially for commercial and law enforcement purposes.[6] This concern was highlighted when it was revealed that Tesla Motors recorded data during a test drive of one of its vehicles by a reporter and used data related to the driver's location, energy usage, speed, temperature and other control settings to rebut the reporter's unfavorable review of

[2] "Adventures in Automotive Networks and Control Units," Dr. Charlie Miller and Chris Valasek, http://illmatics.com/car_hacking.pdf

[3] http://www.npr.org/blogs/alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New-Doors-To-Smarter-Thieves

[4] "Black Hat 2014: Hacking the Smart Car," Mark Anderson, IEEE Spectrum, http://spectrum.ieee.org/cars-that-think/transportation/systems/black-hat-2014-hacking-the-smart-car

[5] See "Researchers Show How a Car's Electronics Can Be Taken Over Remotely," John Markoff, The New York Times, March 9, 2011, http://www.nytimes.com/2011/03/10/business/10hack.html http://www.autosec.org/pubs/cars-oakland2010.pdf and http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[6] "Dash is Turning Cars into Futurists, Data-Collecting Machines with an App and a Cheap Plastic Dongle", Alyson Shontell, Business Insider, http://www.businessinsider.com/a-tiny-piece-of-hardware-turns-your-vehicle-into-a-smart-car-that-talks-and-collect-tons-of-data-2013-8

his driving experience.[7] Car dealerships and navigation systems providers have also begun to use "remote disabling", which enable them to track and disable vehicles if drivers do not keep up with their payments[8] or if cars have been reported as stolen, which can raise safety concerns if the vehicles are disabled during an emergency or when the driver is left stranded in an unsafe location.

Furthermore, vehicle-to-vehicle (V2V) technologies are emerging as a viable tool for improving active safety through collision avoidance, and one of the main unknowns in their development is a robust communication security system.[9] As vehicles continue to become more integrated with wireless technology, there are more avenues through which a hacker could introduce malicious code, and more avenues through which a driver's basic right to privacy could be compromised. These threats demonstrate the need for robust vehicle security policies to ensure the safety and privacy of our nation's drivers.

In order to better understand the ability of automobile companies to protect the safety and privacy of drivers, letters were sent to 20 major automobile manufacturers with questions regarding technology, security precautions, and privacy policies. The questions posed were identical for each manufacturer. Responses were received from 16 manufacturers. Tesla Motors, Aston Martin, and Lamborghini, did not respond to the letters. Volkswagen and Audi responded with a single letter and are together treated in the findings as a single responding manufacturer. Some manufacturers (notably Hyundai and Toyota) provided detailed, question-by-question responses, while others (notably Mercedes-Benz and Porsche) wrote generic statements on their commitments to security and privacy that were non-responsive to the questions that were posed.

Recently, and as a result of the questions posed by Senator Markey, the automobile industry has acknowledged the deficiencies and inconsistences between manufacturers in existing practices for vehicle privacy protections by issuing its own set of voluntary privacy principles.[10] These voluntary principles were developed and supported by the Alliance of Automobile Manufacturers and the Association of Global Automakers, which combined represent 23 major automobile manufacturers, including all of the manufacturers that responded to Senator Markey with the exception of Audi. The adopted principles include (1) transparency, (2) choice, (3) respect for context, (4) data minimization, de-identification and retention, (5) data security, (6) integrity and access, and (7) accountability. The establishment of these principles, and the agreement to them by 19 manufacturers (including all of those that responded to Senator Markey's letter with the exception of Jaguar Land Rover), represent an important step forward by the automotive industry.

Through the voluntary principles, the automakers assure consumers that they will be informed when data collection occurs and given choices regarding whether their information can be used for marketing purposes, companies will not pass on any information to law enforcement without a warrant or court order, and "reasonable" security measures will be in place to protect data from falling into the wrong hands. However, the principles continue to raise a number of questions regarding how car manufacturers will effectively make their practices transparent to consumers and provide consumers with rights to prevent sensitive data collection in the first place, among other concerns.

The diversity of responses received by Senator Markey shows that each manufacturer is handling the introduction of new technology in very different ways, and for the most part these actions are insufficient to ensure security and privacy for vehicle consumers. Individual automaker responses will not be publicly released due to the proprietary and security-sensitive nature of some of the responses. The following sections summarize the major findings from the analysis of responses conducted by Senator Markey's staff.

[7] See "Elon Musk's Data Doesn't Back Up His Claims of New York Times Fakery", Rebecca Greenfield, The Atlantic Wire, http://www.theatlanticwire.com/technology/2013/02/elon-musks-data-doesnt-back-his-claims-new-york-times-fakery/62149/ and http://www.teslamotors.com/blog/most-peculiar-test-drive

[8] "Late on a Car Loan? Meet the Disabler", Jonathan Welsh, The Wall Street Journal, http://online.wsj.com/article/SB123794137545832713.html,

[9] Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist", Government Accountability Office, GAO-14-13, http://www.gao.gov/assets/660/658709.pdf

[10] "Consumer Privacy Protection Principles, Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc., November 12, 2014, http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163

FINDINGS

Finding #1: Nearly 100% of cars on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions.

Wireless technologies in vehicles are becoming more prevalent as manufacturers have found ways that they can be used to improve safety, performance, and the driver experience. However, wireless technologies also require wireless entry points (WEPs), or ways that vehicle electronics can be accessed remotely. In 2011 a group of researchers showed WEPs in automobiles pose vulnerabilities, and they were able to remotely hack into a vehicle and exploit these vulnerabilities, including engaging in location tracking and eavesdropping, and controlling different features including the locks and brakes.[11]

Of the 16 manufacturers that responded to the letter, 14 provided information on the percentage of model year (MY) 2013 vehicles and the projected percentage of MY 2014 vehicles that have WEPs. Of the 14, 11 indicated that 100% of their vehicles have WEPs, and some of these manufacturers cited the federal mandate for tire pressure monitoring systems (TPMS) as a major contributor. Of the 3 who did not indicate that all vehicles have WEPs, the reported percentages of vehicles without WEPs were low, ranging from 7% to 30% and either stagnant or decreasing from 2013 to 2014.

These responses show that nearly all vehicles on the road have at least one WEP, and many vehicles have several WEPs. These include but may not be limited to TPMS, Bluetooth, keyless entry, remote start, navigation, Wi-Fi, cellular/telematics, radio, and anti-theft systems and features.

Finding #2: Most automobile manufacturers were unaware of or unable to report on past hacking incidents.

Senator Markey asked each of the manufacturers to list and describe instances in which they have been made aware of wireless or non-wireless infiltration events in their vehicles. Of the 16 manufacturers who responded to the letter, Jaguar Land Rover, Porsche, and Volkswagen did not respond to the question in any way. Of the 13 companies who did address the issue, 12 stated that they had no knowledge of any reported infiltration events, and only 1 reported such instances. This company described the following in detail:

- An application was developed by a third party and released for Android devices that could integrate with a vehicle through the Bluetooth connection. A security analysis did not indicate any ability to introduce malicious code or steal data, but the manufacturer had the app removed from the Google Play store as a precautionary measure.
- Some individuals have attempted to reprogram the onboard computers of vehicles to increase engine horsepower or torque through the use of "performance chips". Some of these devices plug into the mandated onboard diagnostic port or directly into the under-the-hood electronics system.

Finding #3: Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across all automobile manufacturers, and many manufacturers did not seem to understand the questions posed by Senator Markey.

Manufacturers were asked how they assess their security against WEP infiltration, whether they use third-party testing to verify security, and how they handle software updates associated with recalls and service campaigns to ensure that these are done securely. The questions specifically asked about vulnerabilities associated with tire pressure monitoring systems, Bluetooth/wireless communications technologies, Onstar/navigation systems, smart phone/mobile device integration, web browsers, electronic control units (ECUs), and vehicle-to-vehicle communication technologies.

Of the 16 automobile manufacturers that responded to the letter, 13 of them addressed these questions in some way. Chrysler, Mercedes-Benz, and Mazda did not respond to the question at all, and five other manufacturers provided general responses that addressed the question as a whole instead of providing specific responses to the questions' sub-parts.

[11] "Researchers Show How a Car's Electronics Can Be Taken Over Remotely", John Markoff, The New York Times, March 9, 2011, http://www.nytimes.com/2011/03/10/business/10hack.html

This question seems to have been interpreted differently by different manufacturers. About half of the responses described security or encryption measures for general or specific WEPs that were more related to ensuring the WEPs were working as intended but not to ensuring that a security breach could not occur, and the other half mentioned procedures used in their development process to conduct targeted evaluations of their security measures. The responses revolving around security and encryption measures varied widely from manufacturer to manufacturer, and included the following:

1. Unique identification numbers and specific sets of radio-frequency signals;
2. Receptor to determine frequency strength of sensors to allow for proximity of legitimate communications;
3. Encrypted codes and dedicated wireless devices;
4. Encryption, masking, scanning, anomaly detection, certificates, filtering, firewalls, data loss prevention, access control, intrusion detection systems, white listing, fraud detection, zoning, network segregation and proprietary communication tools;
5. Closed systems where the implementations do not allow the ability for code to be written without authorized tools;
6. Secure Sockets Layer to encrypt the data of network connections;
7. Seed-key security to protect against unauthorized access to the ECU.

Automobile security experts consulted by Senator Markey's staff said that unique ID numbers and radio frequencies (responses 1, 2) can be identified by hackers, that closed system codes (responses 3, 5) have been proven to be re-writable, and seed-key security (response 7) is easily bypassed.

The other half of the responses named procedures utilized in the development process that manufacturers use to ensure WEP security, which was more in line with the wording and intent of the question. These responses included the following steps:

- Threat modeling;
- Penetration testing;
- Input validation and verification;
- Virtual testing;
- Component testing;
- Physical testing.

Seven of the manufacturers stated that they use third-party testing to verify their security measures, while 5 stated that they do not and 4 did not respond to this part of the question.

Automakers were also asked about the number of safety recalls and service campaigns issued by the manufacturers over the five-year period from 2009-2013 and whether those recalls or service campaigns involved software updates that could be used to introduce malware. Chrysler, Mercedes-Benz, Porsche, and Volkswagen did not respond, with the other 12 companies provided different levels of detail in their responses. The responses ranged from 27-210 combined recall or campaign events during that five-year period, with 11-44% of those including software updates of some kind, all of which were delivered using a hardwire connection (not over-the-air like some mobile phone updates are delivered) through a dealer or service center.

The manufacturers were also asked about how they secure this type of software delivery. Each manufacturer responded with descriptions of how they provide such software through authorized dealers with the appropriate tools. Automobile security experts consulted by Senator Markey's staff said that all of the responses are similar in that they presume a malicious actor could not access or acquire the technologies that mechanics have. They state that software updates for systems should be cryptographically verified by the ECU being updated in order to effectively prevent intrusions.

Finding #4: Only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time, and most say they rely on technologies that cannot be used for this purpose at all.

When asked about how manufacturers are capable of monitoring electronic systems in real-time in order to detect and respond to potential intrusions, most of the responses described systems that can only record information on-board the vehicle. This means that infiltrations would only come to the attention of the manufacturer if that data were manually downloaded by a dealer or service center at some subsequent date. When asked about how they would respond to an infiltration, most manufacturers did not respond or mentioned generic security systems in place. Only two manufacturers described credible real-time reactions to an intrusion event.

The manufacturers were asked whether they include technologies to monitor vehicle CAN buses

(the "controller area networks" that manage the communications among the different electronic systems in a vehicle) and to monitor WEPs. They were then asked about how they would respond to reports or detection of an unauthorized intrusion, a remote attack, or inadvertent introduction of malicious code to a WEP. Only eight of sixteen manufacturers responded to these questions, six of which claim to do CAN bus monitoring and five of which claim to be able to detect wireless intrusions. The other 2 manufacturers who responded to the question admitted that they do not monitor the CAN bus, but they are developing systems to do so. Of the other eight companies, Mercedes-Benz, Nissan, and Porsche did not respond at all, and five other manufacturers stated that such information was confidential.

The responses received varied in level of detail and in their methods of monitoring CAN buses. The six manufacturers who claim to monitor CAN buses cited the following:

1. One manufacturer claimed to have a proprietary system that cannot be disclosed;
2. Two manufacturers claimed that the electronic control unit (ECU) is equipped with; monitoring systems that can detect unusual signals, which would alert the manufacturer only if the data were later retrieved at a service center or dealership;
3. One manufacturer described a firewall and watchdog system that shields communication and recognizes inconsistencies at gateways;
4. One manufacturer listed message authentication, intrusion detection, controller hardening protection, secure diagnostics, secure gateways, and secure programming;
5. One manufacturer mentioned that seed-key security is applied to protect vehicles from unauthorized access, which generates a random security variable which must be matched in order to allow communication access.

Automobile security experts consulted by Senator Markey's staff noted that the ECU monitoring (response 2) and firewall/watchdog systems (response 3) would only check for unusual network behavior and not detect any problems with the data itself. An analogy was given to compare it to somebody receiving threatening phone calls, where the phone company is monitoring the lines to see if phone calls are getting through, but not checking the content of the conversations. They also noted that the seed-key system (response 5) could be bypassed by malicious actors.

The question of monitoring WEPs for intrusions received similar responses. Of the eight manufacturers that responded:

1. Four manufacturers mentioned that some of the features themselves are equipped with encryption and security technologies;
2. One manufacturer mentioned continuous ECU monitoring (also above);
3. One manufacturer described the firewall/watchdog system (also above);
4. One manufacturer described the seed-key security system (also above);
5. One manufacturer stated that its remote keyless entry systems can record key code authentication failures.

The encryption and security measures (response group 1) are not systems that can detect intrusion events. Automobile security experts consulted by Senator Markey's staff have noted that the ECU monitoring (response 2) described simply monitors the normal functioning of an ECU, the firewall/watchdog systems (response 3) would only protect against random outside influences like electromagnetic frequency interference and not malicious intrusions, the seed-key system (response 4) can be defeated by hackers, and the remote keyless entry systems (response 5) will only protect against people getting into the car to steal it but will do nothing to prevent or respond to remote hacking. Also, only 1 of the systems, the seed-key system, is capable of alerting the manufacturer in real-time.

Finally, on the question of how the manufacturers would respond to an intrusion in real-time, six of the manufacturers did not respond, and six more responded with vague mentions of security systems and "taking appropriate actions" such as recalls and service campaigns that could not be used to respond in real-time. The other four manufacturers provided the following responses:

1. One manufacturer claimed that it would contact the subscriber through the telematics program to alert them and resolve any problems;
2. One manufacturer said that it has the ability to disable certain connected features;
3. One manufacturer claimed that it could place a vehicle in a "fail-safe" mode that may limit vehicle operation if malfunctions that could cause damage occur;

4. One manufacturer stated that it would have the option to safely slowdown and immobilize an impacted vehicle if the vehicle is in motion at the time of detection.

The first 2 of these responses, contacting through the telematics program or disabling features, would not be an effective real-time way to deal with an ongoing attack, according to automobile security experts consulted by Senator Markey's staff. Responses 3 and 4, fail-safe mode and remote slowdown and immobilization, are the only responses that indicate an ability to immediately respond to security threats and address the situation for the drivers who subscribe to their telematics providers.

These three questions and their responses have revealed that, of the manufacturers who were willing to respond, only one of them appears to be able to detect wireless intrusions, and only one or two have described credible means of responding to such intrusions in real time.

Finding #5: Automobile manufacturers collect large amounts of data on driving history and vehicle performance.

New vehicles are capable of collecting a tremendous amount of data through a variety of pre-installed technological systems. Senator Markey's letter asked manufacturers about (1) what types of navigation technology or other technologies are in their vehicles with the ability to collect driving history information, (2) what percentage of U.S. automobiles contain such technologies in MY2013 and MY2014, and (3) what types of information can be collected. Honda, Porsche, and Mercedes-Benz did not respond to these questions, and the other 13 manufacturers responded with various levels of completeness.

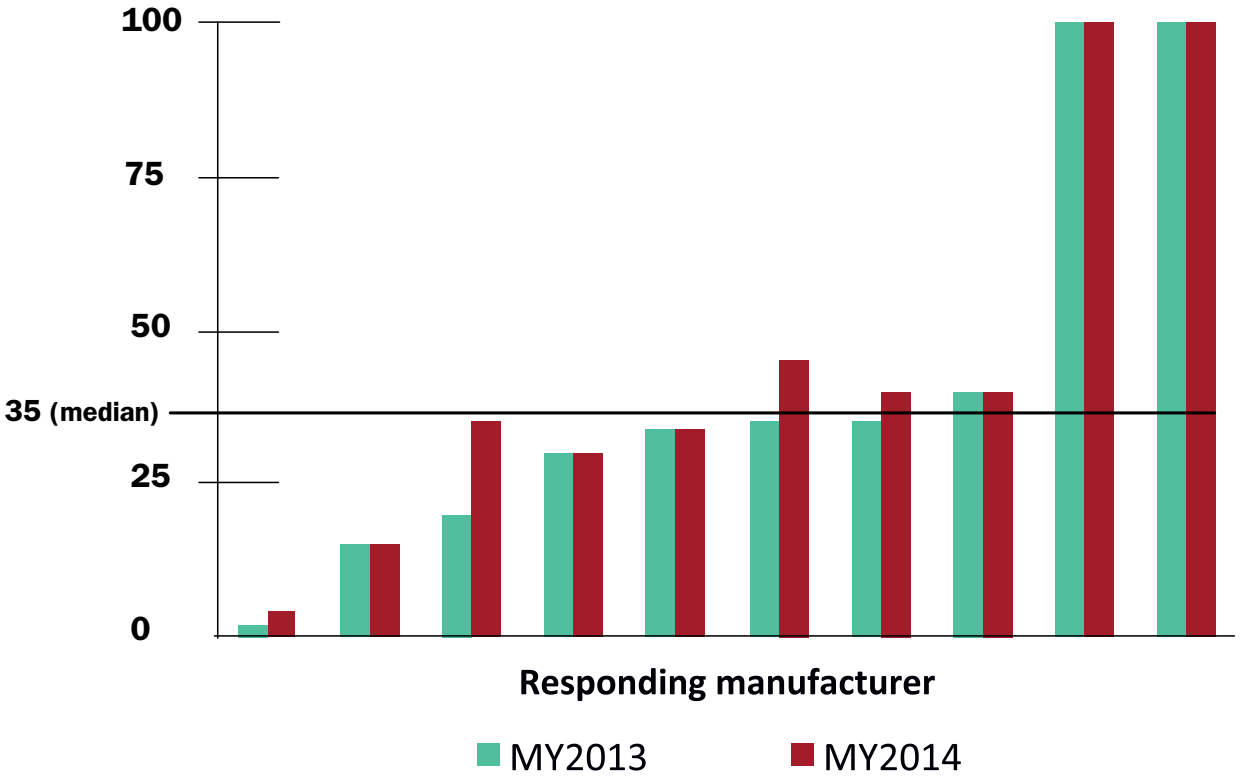
The responses to the first question included a range of navigation, telematics, infotainment, emergency assist, stolen vehicle recovery, and event data recording systems that have the ability to record driving history information. These included branded products like OnStar and SYNC as well as other unbranded technologies, collecting a diverse set of data types that included the following:

- Geographic location (7 manufacturers), such as:
  - Physical location recorded at regular intervals;
  - Previous destinations entered into navigation system;
  - Last location parked.
- System settings for event data recorder (EDR) devices (5 manufacturers), which can include:
  - Potential crash events, such as sudden changes in speed;
  - Status of steering angle, brake application, seat belt use, and air bag deployment;
  - Fault/error codes in electronic systems.
- Operational data (7 manufacturers), such as:
  - Vehicle speed;
  - Direction/heading of travel;
  - Distances and times traveled;
  - Average fuel economy/consumption;
  - Status of power windows, doors, and locks;
  - Tire pressure;
  - Fuel level;
  - Tachometer reading (engine RPM gauge);
  - Odometer reading;
  - Mileage since last oil change;
  - Battery health;
  - Coolant temperature;
  - Engine status;
  - Exterior temperature and pressure.

While three of the manufacturers who responded claimed to not record any driving history information, three others listed all three of the categories above.

The percentages of vehicles that contain such technologies varied greatly among the manufacturers, with some claiming that almost no vehicles have them while others claim that all of their vehicle models do. The percentages are shown in the chart below, with a median response of 35% of vehicles from a manufacturer containing technologies that can collect driving history information. These percentages either showed slight increases or stagnation from MY2013-MY2014.

PERCENTAGE OF VEHICLES THAT CAN RECORD DRIVING HISTORY



The two coalitions of manufacturers recently adopted voluntary privacy principles—namely on "data minimization, de-identification, and retention" that attempt to address these concerns. On minimization, this principle states that manufacturers commit to collecting information "only as needed for legitimate business purposes". While this is a good step forward, limiting themselves to collection "only as needed for legitimate business purposes" still raises many questions about the extent to which companies will continue to collect sensitive information. The principles also do not ensure that consumers will have rights to prevent data collection in the first place.

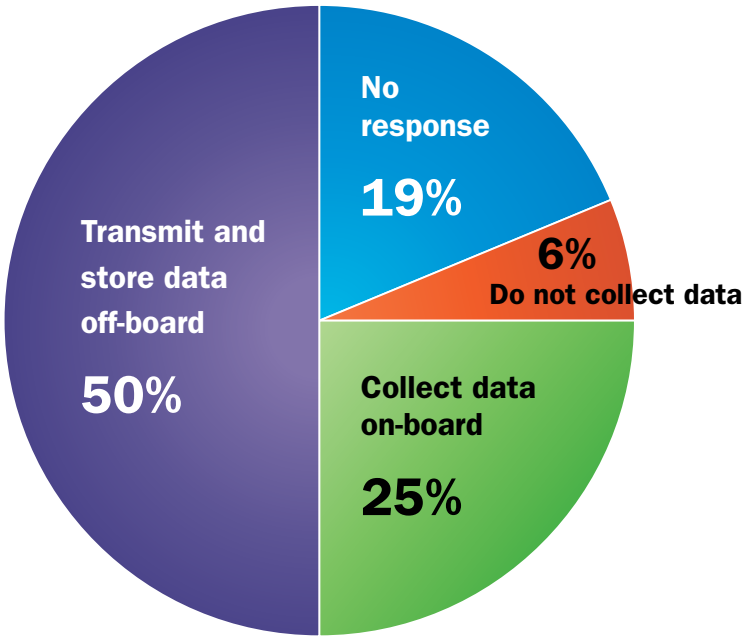
Finding #6: A majority of automakers offer technologies that collect and wirelessly transmit driving history data to data centers, including third-party data centers, and most do not describe effective means to secure the data.

Automobile manufacturers store data in a variety of different ways. Some said that it is only stored on-board the vehicle and cannot be wirelessly retrieved, and others described how they wirelessly transfer all data to a central location (known as off-board storage). Also, the large majority of the companies who responded (9 of 11) claimed that they do contract with third-party companies to provide the data-collecting features that they offer. In fact, 3 manufacturers specifically stated they license third party companies to transmit and store data associated with the features.

To the question of whether driving history information is recorded and stored in a vehicle, 12 manufacturers replied that they do store this information in some of their vehicles (depending on the features the vehicle is equipped with). Only 1 manufacturer stated that they do not collect such data, and 3 did not respond. This indicates that an overwhelming majority of vehicles collect driving history information.

Of the 12 who said they collect and store driving history data, 8 stated that they transmit and store driving history data in a server off-board the vehicle, while the other 4 stated that they do not. This reveals that a majority of vehicle manufacturers offer features that not only record but also transmit driving history wirelessly to themselves or to third parties.

PERCENTAGE OF AUTOMOBILE MANUFACTURERS THAT COLLECT AND TRANSMIT DRIVING HISTORY DATA



Finally, the security measures of these data collection systems vary widely by manufacturer, and in some cases there are none. In the case of on-board storage, no manufacturer described any security system to protect that data, and several of them noted that no security measure is needed since accessing data would require a hardwire connection. Regarding security measures to protect data that is wirelessly transmitted outside the vehicle, only 6 responses were received. Of those, 5 provided vague responses naming encryption, passwords, or general IT security practices, and only 1 specifically mentioned that they designed their systems to limit the transfer of personally identifiable information.

The automakers' voluntary privacy protection principles include commitments to "respect for context" and "data security". The "respect for context" principle addresses the ways that data are collected and shared, and it provides a list of examples to illustrate "reasonable and responsible ways" that automakers may collect and share data with both affiliated companies and non-affiliated entities. These include, among others, providing subscribed services, conducting research, responding to emergencies and faults, sharing for operational purposes, and complying with lawful government requests—describing a sweeping suite of practices and offering no specific guidelines for reducing data collection and sharing.

The "data security" principle states that the automakers commit to collecting information "only as needed for legitimate business purposes", which is another positive message toward reducing unneeded sharing of information. However, this principle offers no detail as to what may be included under "legitimate business purposes", effectively leaving it open for interpretation by the coalition members.

Finding #7: Manufacturers use personal vehicle data in various ways, often vaguely to "improve the customer experience" and usually involving third parties, and retention policies—how long they store information about drivers—vary considerably among manufacturers.

A wide array of responses was received regarding the ways that manufacturers use vehicle history information. Of the 8 manufacturers that previously stated that they collect such information, 3 of them did not respond to this question, with the other five listing combinations of the following uses:

- Provide feature functionality;
- Maintain and improve services;
- Address vehicle safety concerns;
- Diagnose and assist with technical issues;
- Respond when the system senses the vehicle has been involved in an accident;
- Fulfill requests for service by customers;
- Research purposes (analytics and marketing).

Many of these responses are vague and not well-defined, such as providing feature functionality, maintaining and improving services, and serving research purposes. This lack of transparency in personal vehicle data usage leaves consumers with little knowledge about how the companies actually use their data.

Additionally, the letters revealed that 5 of the 8 manufacturers claimed to share this information with third parties to provide subscriber services. All of them stated that they do not sell such information, and 2 specifically mentioned that they do not share any personally identifiable information. This reveals that a majority of manufacturers who collect data share that information with third party companies.

Another question that received a wide range of responses was about how long driving history data is retained in the various systems that record and store them. To this question, four of the twelve manufacturers did not answer, with the other eight providing responses that sometimes varied by feature/technology. These ranged from responses that information is retained no longer than a year, to responses that indicate that information is retained indefinitely.

- Five manufacturers listed that information is deleted after a set period of time, ranging from one to ten years;
- Three manufacturers replied that there is no set clear date, with two of them stating that it can be deleted by users at any time;
- One manufacturer stated that navigation information is overwritten when the system runs out of memory storage space;
- One manufacturer said that on-board error information is deleted when the vehicle fault is cleared.

The new industry-led voluntary privacy principles include a commitment by automakers to only collect data "as needed for legitimate business purposes" and to retain identifiable or personal subscription

information "no longer than they determine necessary for legitimate business purposes". The intention of this principle is positive, but these limitations are subject to the interpretation of the industry and offer no explicit rules to prevent excessive collection or retention. Regarding the ways in which data are used, the coalitions put forth the "respect for context" principle, which describes a list of "reasonable and responsible ways" that members can use or share data collected from vehicles. This includes an important provision that a warrant or court order is needed if companies are to share geolocation information with law enforcement. Unfortunately, however, this broad proclamation provides little tangible assurances that consumers will not disapprove of the ways in which manufacturers use their sensitive information.

Additionally, the automakers' voluntary "choice" principle specifically requires affirmative consent from the consumer before sharing sensitive driving history data, specifically geolocation, biometric, and driver behavior information, for marketing purposes or with unaffiliated third parties. However, this commitment fails to address whether a consumer's decision to agree or disagree will affect the functionality of the vehicle or the features that are available to them. The principles also do not pertain to sharing (1) non-sensitive data for marketing purposes, and (2) sensitive data for non-marketing purposes.

Finding #8: Customers are often not explicitly made aware of data collection and, when they are, they often cannot opt out without disabling valuable features, such as navigation.

The primary methods manufacturers use to inform customers of data collection are by mentioning it in the owners' manual or including it in the terms and conditions of the vehicle sale or specific feature activation. If a customer actually becomes aware of data collection and wishes to disable it, they often must accept a loss of feature functionality, such as GPS.

Of the twelve manufacturers who confirmed that they do record and store data, three did not respond to the question on how customers are made aware of data storage, and one stated that there is no reason to inform users of on-board storage. The other eight manufacturers listed combinations of the following methods of notice:

- Owners' manuals;
- Privacy statements;
- Terms & Conditions (which must be "accepted").

To the question of whether and how customers can disable data collection or transmission, four did not respond. Two manufacturers said that users cannot disable data collection, two said that they can disable it, and four stated that it is possible by turning off a feature or canceling a service subscription.

On the question of whether users (if they are made aware of data collection) can delete information, six manufacturers did not respond, five specifically noted that customers can delete data directly through the navigation system interface, and one mentioned that customers can request data deletion by contacting the service provider.

These responses show that customer awareness of data collection is primarily distributed within long written texts such as Terms & Agreement statements or owner manuals. In the event that customers read these and are aware of them, they do, in certain cases, have the ability to delete previously-recorded data. However, disabling the constant collection of data often requires disabling valuable vehicle features or services.

The new voluntary privacy principles from the manufacturers partially address these concerns with commitments to "transparency" and "choice". Signing members agree to provide consumers "with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing" of data. This includes a list of ways that manufacturers can provide these notices, which include "owners' manuals, on paper or electronic registration forms and user agreements, or on in-vehicle displays". Unfortunately, these types of notices likely do not guarantee an improvement over current practices revealed in the responses to Senator Markey, as most manufacturers claimed that such notices are already provided in user manuals and terms & conditions that must be signed upon purchase.

Regarding choice, the principle states that consumers must give "affirmative consent", or opt in, when certain information such as geolocation, biometrics, or driver behavior is collected or shared for marketing or with unaffiliated third parties. The principle does not commit manufacturers to offering consumers the option to prevent data collection in the first place or giving consumers the choice to remove data that have already been collected. Additionally, consumers who choose not to consent to data collection may be denied access to valuable vehicle features. For instance, consent to sharing geolocation information for marketing purposes may be the only way for a consumer to turn on the navigation feature.