STANLEY LAW GROUP
MATTHEW J. ZEVIN, SBN: 170736
10021 Willow Creek Road, Suite 200
San Diego, CA 92131
Telephone: (619) 235-5306
Facsimile: (815) 377-8419
e-mail: mzevin@aol.com

STANLEY LAW GROUP
MARC R. STANLEY, Texas SBN: 19046500
Admitted *Pro Hac Vice*
MARTIN WOODWARD, Texas SBN: 00797693
Admitted *Pro Hac Vice*
6116 North Central Expressway, Suite 1500
Dallas, TX 75206
Telephone: (214) 443-4300
Facsimile: (214) 443-0358
e-mail: marcstanley@mac.com
mwoodward@stanleylawgroup.com

Attorneys for Plaintiffs
[Additional Counsel Listed on Signature Page]

IN THE UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN FRANCISCO DIVISION

HELENE CAHEN, KERRY J. TOMPULIS, and MERRILL NISAM, RICHARD GIBBS, and LUCY L. LANGDON, on Behalf of Themselves and All Others Similarly Situated,

Plaintiffs,

v.

TOYOTA MOTOR CORPORATION, TOYOTA MOTOR SALES, U.S.A., INC., FORD MOTOR COMPANY, GENERAL MOTORS LLC, and DOES 1 through 50,

Defendants.

CASE NO. 15-cv-01104-WHO

FIRST AMENDED COMPLAINT FOR BREACH OF WARRANTY, BREACH OF CONTRACT, FRAUD, FRAUDULENT CONCEALMENT, INVASION OF PRIVACY AND VIOLATION OF CONSUMER PROTECTION LAWS

CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiffs Helene Cahen, Kerry J. Tompulis, Merrill Nisam, Richard Gibbs, and Lucy L. Langdon ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class"), allege as follows:

INTRODUCTION

1. Some automobile manufacturers have chosen to manufacture and sell cars that rely heavily on computer technology. In choosing to add this technology to their cars, Defendants Toyota Motor Corporation and Toyota Motor Sales, U.S.A., Inc. (together, "Toyota"), Ford Motor Company ("Ford"), and General Motors LLC ("GM") assumed a very significant responsibility: the obligation to keep drivers and passengers safe from harm, even though the computer technology in the cars is exposed to the dangers of being "hacked"—infiltrated and taken over by third parties. Such "hacking" can result in loss of driver authority over the throttle, braking and steering of the vehicle, as well as loss of personal and private data.

2. But Toyota, Ford, and GM did not think through the consequences of their actions. These three automakers essentially turned their cars into smartphones on wheels—but used ancient, outmoded technology with known vulnerabilities that make the cars highly susceptible to hacking and, therefore, unreasonably dangerous. Because Defendants failed to ensure the basic electronic security of their vehicles, control of the basic functions of the vehicle can be taken by others not behind the wheel or necessarily even in the car, which can endanger the safety of the driver and others.

3. This is because Defendants' vehicles contain dozens of electronic control units (ECUs) that are connected through an insecure controller area network (typically a "CAN" or "CAN bus"). Vehicle functionality and safety depend on the proper functioning of these small computers, which depends in part on the reliability of their communications.

4. The ECUs communicate by sending each other "CAN packets," which are digital messages containing data and/or requests. But if an outside source, such as a hacker, were able to send CAN packets to ECUs on a vehicle's CAN bus, the hacker could confuse one or more ECUs and thereby, either temporarily or permanently, take control of basic functions of the vehicle away from the driver.

5. Disturbingly, as Defendants have known, their controller area network bus-equipped vehicles, when connected to integrated cell phone systems or a Class 1 or Class 2 master Bluetooth device[1] are susceptible to hacking, and their ECUs cannot detect or stop hacked CAN packets. For this reason, Defendants' vehicles are not secure, and are therefore not safe.

6. As a result of Defendants' unfair, deceptive, and/or fraudulent business practices, and their failure to disclose the highly material fact that their vehicles are susceptible to hacking and neither secure nor safe, owners and/or lessees of Defendants' vehicles are currently at risk of theft, damage, serious physical injury, or death as a result of hacking, and they will continue to face this risk until they are notified of the dangers associated with their vehicles and are given funds and guidance by Defendants as to how to correct the security defects, or until Defendants correct them.

7. Moreover, unbeknownst to the owners and/or lessees of Defendants' vehicles, Defendants are remotely collecting data from the vehicles. Even though drivers have a reasonable expectation of privacy as to such data, Defendants share it with or sell it to third parties, often without adequate security (making it an attractive target for hackers). This violates the privacy rights of the owners and lessees.

8. Toyota manufactures and sells vehicles under the Toyota, Lexus, and Scion names (the "Toyota Vehicles"); Ford manufactures and sells vehicles under the Ford, Lincoln, and (until 2011) Mercury names (the "Ford Vehicles"); GM manufactures and sells vehicles under the Buick, Cadillac, Chevrolet, and GMC names (the "GM Vehicles").[2] The computerized components in all Toyota Vehicles, Ford Vehicles, and GM Vehicles are essentially identical in that they are all susceptible to hacking when connected with integrated cell phone systems or a Class 1 or Class 2 master Bluetooth and thus suffer from the same defect. For purposes of this

/./.

[1] Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz[4]) from fixed and mobile devices, and building personal area networks (PANs). Class 1 has a range of 66-98 feet and Class 2 has a range of 16-33 feet. https://en.wikipedia.org/wiki/Bluetooth (last accessed June 30, 2015).

[2] The term "GM Vehicles" as used in this Complaint only includes vehicles manufactured and sold by GM on or after July 10, 2009.

Complaint, all Toyota Vehicles, Ford Vehicles, and GM Vehicles equipped with computerized components are referred to collectively as the "Class Vehicles" or "Defective Vehicles."

9. Plaintiffs bring this action individually and on behalf of all other current and former owners or lessees of Toyota Vehicles, Ford Vehicles, and GM Vehicles equipped with computerized components that are connected via a controller area network to an integrated cell phone or Class 1 or Class 2 master Bluetooth device. Plaintiffs seek damages, injunctive relief, and equitable relief for the conduct of Defendants, as alleged in this complaint.

JURISDICTION

10. This Court has jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the proposed Class consists of 100 or more members; the amount in controversy exceed $5,000,000, exclusive of costs and interest; and minimal diversity exists. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

VENUE

11. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District. Plaintiffs Cahen and Nisam purchased Class Vehicles in this District, and Defendants have marketed, advertised, sold, and leased the Class Vehicles within this District.

PARTIES

12. Plaintiff Helene Cahen is an individual residing in Berkeley, California. In September 2008, Plaintiff Cahen purchased a new 2008 Lexus RX 400 H from an authorized Lexus dealer in San Rafael, California. Plaintiff Cahen still owns this vehicle.

13. Plaintiff Kerry J. Tompulis is an individual residing in Beaverton, Oregon. In August 2014, Plaintiff Tompulis leased a new 2014 Ford Escape from Landmark Ford, an authorized Ford dealer in Tigard, Oregon. Plaintiff Tompulis still leases this vehicle.

14. Plaintiff Merrill Nisam is an individual residing in Mill Valley, California. In March 2013, Plaintiff Nisam purchased a new 2013 Chevrolet Volt from Novato Chevrolet, an authorized Chevrolet dealer in Novato, California. Plaintiff Nisam still owns this vehicle.

/./.

15. Plaintiffs Richard Gibbs and Lucy L. Langdon are individuals residing in Sequim, Washington. In 2014, Plaintiffs Gibbs and Langdon purchased a pre-owned 2013 Ford Fusion from Sound Ford, an authorized Ford dealer in Renton, Washington. Plaintiffs Gibbs and Langdon still own this vehicle.[3]

16. Defendant Toyota Motor Corporation ("TMC") is a Japanese corporation. TMC is the parent corporation of Toyota Motor Sales, U.S.A., Inc. TMC, through its various entities, designs, manufactures, markets, distributes and sells Toyota, Lexus and Scion automobiles in California and multiple other locations in the United States and worldwide.

17. Defendant Toyota Motor Sales, U.S.A., Inc. ("TMS") is incorporated and headquartered in California. TMS is Toyota's U.S. sales and marketing arm, which oversees sales and other operations in 49 states, and specifically in the states of California, Washington and Oregon. TMS distributes Toyota, Lexus and Scion vehicles and sells these vehicles through its network of dealers.

18. Money received from the purchase of a Toyota Vehicle from a dealer flows from the dealer to TMS. Money received by the dealer from a purchaser can be traced to TMS and TMC.

19. TMS and TMC sell Toyota Vehicles through a network of dealers who are the agents of TMS and TMC.

20. TMS and TMC are collectively referred to in this complaint as "Toyota" or the "Toyota Defendants" unless identified as TMS or TMC.

21. At all times relevant to this action, Toyota manufactured, sold, leased, and warranted the Toyota Vehicles at issue under the Toyota, Lexus, and Scion names throughout the United States. Toyota and/or its agents designed, manufactured, and installed the defective CAN buses in the Toyota Vehicles. Toyota also developed and disseminated the owner's manuals and warranty booklets, advertisements, and other promotional materials relating to the Toyota Vehicles.

[3] A television news story about this vehicle showing it being compromised and controlled remotely is available for viewing at http://www.king5.com/story/news/2015/05/19/cars-auto-computer-security-hacking/27610967/ (last accessed June 30, 2015).

22. Defendant Ford Motor Company is a corporation doing business in all fifty states (including the District of Columbia), and specifically in the states of California, Washington and Oregon and is organized under the laws of the State of Delaware, with its principal place of business in Dearborn, Michigan.

23. At all times relevant to this action, Ford manufactured, sold, leased, and warranted the Ford Vehicles at issue under the Ford, Lincoln, and (until 2011) Mercury names throughout the United States. Ford and/or its agents designed, manufactured, and installed the defective CAN buses in the Ford Vehicles. Ford also developed and disseminated the owner's manuals and warranty booklets, advertisements, and other promotional materials relating to the Ford Vehicles.

24. Defendant General Motors LLC is a limited liability company formed under the laws of the State of Delaware with its principal place of business in Detroit, Michigan. GM was incorporated in 2009 and on July 10, 2009 acquired substantially all assets and assumed certain liabilities of General Motors Corporation through a Section 363 sale under Chapter 11 of the U.S. Bankruptcy Code.

25. At all times relevant to this action, GM manufactured, sold, leased, and warranted the GM Vehicles[4] at issue under the Buick, Cadillac, Chevrolet, and GMC names throughout the United States, and specifically in the states of California, Washington and Oregon. GM and/or its agents designed, manufactured, and installed the defective CAN buses in the GM Vehicles. GM also developed and disseminated the owner's manuals and warranty booklets, advertisements, and other promotional materials relating to the GM Vehicles.

TOLLING OF THE STATUTE OF LIMITATIONS

26. Any applicable statute(s) of limitations has been tolled by Defendants' knowing and active concealment and denial of the facts alleged herein. Plaintiffs and the other Class members could not have reasonably discovered the true, latent defective nature of the CAN buses until shortly before this class action litigation was commenced.

/./.

[4] As set forth *supra* n.2, the term "GM Vehicles" only includes vehicles manufactured and sold by GM on or after July 10, 2009, and does not include any vehicle manufactured and sold before that date by General Motors Corporation.

27. Defendants were and remain under a continuing duty to disclose to Plaintiffs and the other Class members the true character, quality, and nature of the Class Vehicles, that this defect is a result of Defendants' design choices, and that it will require costly repairs, and diminishes the resale value of the Class Vehicles. As a result of the active concealment by Defendants, any and all statutes of limitations otherwise applicable to the allegations herein have been tolled.

FACTUAL ALLEGATIONS

How Defendants' Computerized Vehicles Work

28. Many modern automobiles, including the Class Vehicles, contain a number of different networked electronic components that together monitor and control the vehicle. Class Vehicles each contain dozens of electronic control units ("ECUs"), many of which are networked together on a controller area network (typically a "CAN" or "CAN bus").[5] Crucially, the overall safety of the vehicle relies on near real time communication between these various ECUs.[6]

29. As stated by two researchers in a 2013 study funded by the U.S. Defense Advanced Research Projects Agency ("DARPA"): "Drivers and passengers are strictly at the mercy of the code running in their automobiles and, unlike when their web browser crashes or is compromised, the threat to their physical well-being is real."[7]

30. ECUs networked together on one or more CAN buses communicate with one another by sending electronic messages comprised of small amounts of data called CAN packets.[8] These CAN packets are broadcast to all components on a CAN bus, and each ECU decides

/./.

[5] Other such networks are LINBus, MOST, Flexray, and Ethernet. *See* Craig Smith, *Car Hackers 2014: Owner's Manual* at 21.

[6] *Tracking & Hacking: Security & Privacy Gaps Out American Drivers at Risk*, A report written by the staff of Senator Edward J. Markey (D-Massachusetts), http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (last accessed June 30, 2015) (hereinafter "Markey Report") at 3 (a true and correct copy of the Markey Report is attached hereto as Exhibit 1); *see also* Dr. Charlie Miller & Chris Valasek, Technical White Paper: *Adventures in Automotive Networks and Control Units*, http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf (last accessed June 30, 2015) (hereinafter "Miller & Valasek") at 5, 7-8.

[7] Miller & Valasek at 4; *see also* Markey Report at 3.

[8] Miller & Valasek at 4.

whether it is the intended recipient of any given CAN packet. Notably, there is no ECU source or authentication, nor any encryption, built into CAN packets.

31. As described by one commentator: "Consider the level of complexity of modern day cars—and the chance for a screw up. The space ship that put humans on the moon, Apollo 11, had 145,000 lines of computer code. The Android operating system has 12 million. A modern car? Easily 100 million lines of code."[9]

Defendants' Computerized Vehicles Are Susceptible to Dangerous Hacking

32. The CAN standard was first developed in the mid-1980s and is a low-level protocol which does not intrinsically support any security features.[10] Companies that employ CAN busses must deploy their own security mechanisms with higher protocol layers; e.g., to authenticate senders and prevent man-in-the-middle and replay attacks.[11]

33. Lacking security, an automobile reliant upon CAN packets for safety is exposed to hacking that injects one or more false messages onto a CAN bus or manipulates packets in transit on the network.[12] This capability can be used maliciously by anyone with physical access to a CAN bus equipped vehicle.

34. Moreover, wireless interfaces dramatically increase the attack surface in a vehicle by allowing anyone capable of connecting to such a wireless interface to thereby gain access to the CAN bus to invade a user's privacy, by observing CAN packets, and/or inject or modify CAN packets to take remote control of the operation of a vehicle. For example, a vehicle equipped with a Bluetooth wireless interface is susceptible to an attacker remotely and wirelessly accessing the vehicle's CAN bus through Bluetooth connections.[13] An even greater risk exists with an integrated cell phone connected to the CAN bus. Vehicles equipped with OnStar (GM), Entune

/./.

[9] Jose Paglieri, *Your Car Is A Giant Computer—And It Can Be Hacked*, http://money.cnn.com/2014/06/01/technology/security/car-hack/ (last accessed June 30, 2015).
[10] http://en.wikipedia.org/w/index.php?title=CAN_bus (last accessed June 30, 2015).
[11] *Id.*
[12] *See* Xavier Aaronson, *We Drove a Car While It Was Being Hacked*, http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked (last accessed June 30, 2015).
[13] Miller & Valasek at 4; *see also* Markey Report at 3.

(Toyota) and other telematics services[14] have such integrated cellular phones. Others, such as those equipped with Sync (Ford)[15] allow the owner or a vehicle occupant to use their own cellular phone to have access to the CAN bus via a Bluetooth connection. Hacking can be accomplished by connecting to such integrated or Bluetooth connected phones, as demonstrated by DARPA in an episode broadcast on CBS 60 Minutes.[16]

35. One journalist described the experience of driving a vehicle whose CAN bus was being hacked remotely (but under controlled circumstances) as follows:

> As I drove to the top of the parking lot ramp, the car's engine suddenly shut off, and I started to roll backward. I expected this to happen, but it still left me wide-eyed.
>
> I felt as though someone had just performed a magic trick on me. What ought to have triggered panic actually elicited a dumbfounded surprise in me. However, as the car slowly began to roll back down the ramp, surprise turned to alarm as the task of steering backwards without power brakes finally sank in.
>
> This wasn't some glitch triggered by a defective ignition switch, but rather an orchestrated attack performed wirelessly, from the other side of the parking lot, by a security researcher.[17]

Defendants Have Known for Years that Their Computerized Vehicles Can Be Hacked

36. These security vulnerabilities have been known in the automotive industry—and, specifically, by Defendants—for years. Researchers at the University of California San Diego and University of Washington had discovered in 2011 that modern automobiles can be hacked in a number of different ways—and, crucially, that wireless interfaces can allow a hacker to take control of a vehicle from a long distance.[18]

/./.

[14] See PRN Newswire Sprint and Ford Team to Deliver In-Vehicle, Integrated, Voice-Activated Wireless Products And Services. http://www.prnewswire.com/news-releases/sprint-and-ford-team-to-deliver-in-vehicle-integrated-voice-activated-wireless-products-and-services-73097807.html (last accessed June 30, 2015).

[15] http://www.ford.com/technology/sync/?ef_id=VRMkYQAAAI14FTX2:20150630122926:s&searchid=67176874|2242383154 (last accessed June 30, 2015).

[16] https://news.cs.washington.edu/2015/02/09/watch-uw-cse-and-darpa-hack-a-car-driven-by-60-minutes-leslie-stahl/ (last accessed June 30, 2015).

[17] Xavier Aaronson, *We Drove a Car While It Was Being Hacked*, http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked (last accessed June 30, 2015).

[18] Stephen Checkoway et al., *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, http://www.autosec.org/pubs/cars-usenixsec2011.pdf (last accessed June 30, 2015).

37. Building on this research, in a 2013 DARPA-funded study, two researchers demonstrated their ability to connect a laptop to the CAN bus of a 2010 Toyota Prius and a 2010 Ford Escape using a cable, send commands to different ECUs through the CAN, and thereby control the engine, brakes, steering and other critical vehicle components.[19] In their initial tests with a laptop, the researchers were able to cause the cars to suddenly accelerate and turn, kill the brakes, activate the horn, control the headlights, and modify the speedometer and gas gauge readings.[20]

38. Before the researchers went public with their 2013 findings, they shared the results with Toyota and Ford in the hopes that the companies would address the identified vulnerabilities.[21] The companies, however, did not.

39. In August of 2014, members of a security research group who had independently studied automobile hacking wrote an open letter to the CEOs of major automobile manufacturers, urging them to work collaboratively with the cyber security industry in making vehicles safe from the threat of hacking.[22] The group proposed a five-point protocol for automobile manufacturers to follow—including such measures as ensuring that vehicles have the capability for security updates, logging and evidence capture (similar to an airplane's "black box"), and segmentation and isolation to ensure that non-critical systems (e.g., Bluetooth) cannot affect critical systems (e.g., brakes or steering) if compromised.[23] Despite the group's elaborate description of known vulnerabilities to the automotive industry CEOs, Defendants have not adopted any of the proposed security protocols that would address the vulnerabilities and make vehicles safer.

/./.

/./.

[19] *See generally* Miller & Valasek.

[20] *See generally* Miller & Valasek. A video of the researchers hacking and taking control of the operation of the cars can be viewed at https://www.youtube.com/watch?v=oqe6S6m73Zw (last accessed June 30, 2015).

[21] Markey Report at 3.

[22] August 8, 2014 letter from "I Am The Cavalry," https://www.iamthecavalry.org/wp-content/uploads/2014/08/IATC-Open-letter-to-the-Automotive-Industry.pdf (last accessed June 30, 2015).

[23] I Am The Cavalry, Five Star Automotive Cyber Safety Framework, https://www.iamthecavalry.org/domains/automotive/5star/ (last accessed June 30, 2015).

40. And, as recently as May of 2015, the general counsel for an automobile industry association (of which Defendant Toyota is a member) acknowledged the imminent eventuality of a remote hacking attack on cars:

> Picture this: you're driving along a stretch of road, and an unseen force takes over. The car picks up speed, then swerves—without your touching the accelerator or turning the wheel. You're no more than a helpless passenger. What just happened? Your car has been hacked.
>
> It's a frightening scenario. But how real is this threat? Real enough that car manufacturers and security experts from the federal government are taking it seriously.
>
> ***"Any cyber expert will tell you that you can't prevent it; it's just a question of when,"*** says Mark Dowd, assistant general counsel for Global Automakers, a coalition of car manufacturers working to combat the looming threat of cyber attacks (emphasis added).[24]

Despite Selling Unsafe Computerized Vehicles, Defendants Tout Their Safety

Toyota

41. Toyota has consistently marketed its vehicles as "safe" and portrayed safety as one of its highest priorities.

42. As Toyota states in one of its promotional materials:

> Toyota believes that the ultimate goal of a society that values mobility is to eliminate traffic fatalities and injuries. Toyota's Integrated Safety Management Concept sets the direction for safety technology development and vehicle development, and covers all aspects of driving by integrating individual vehicle safety technologies and systems rather than viewing them as independently functioning units.[25]

43. In another, Toyota states:

> Pursuit for Vehicle Safety
>
> Toyota has been implementing "safety" measures to help create safer vehicles.[26]

/./.

[24] Jim Travers, *Keeping Your Car Safe from Hacking*, http://www.consumerreports.org/cro/news/2015/05/keeping-your-car-safe-from-hacking/index.htm (last accessed June 30, 2015).
[25] http://www.toyota-global.com/innovation/safety_technology/media-tour/ (last accessed June 30, 2015).
[26] http://www.toyota-global.com/innovation/safety_technology/safety_measurements/ (last accessed June 30, 2015).

44. And in a third, Toyota states:

> Toyota recognizes the importance of the driver being in ultimate control of a vehicle and is therefore aiming to introduce AHDA and other advanced driving support systems where the driver maintains control and the fun-to-drive aspect of controlling a vehicle is not compromised.[27]

Ford

45. Ford similarly markets and promotes its vehicles as "safe." For example, in describing its 2015 Fusion, Ford states:

> Safety
>
> When you look over the impressive list of collision avoidance and occupant protection features, you'll know how well-equipped Fusion is when it comes to you and your passengers' safety.[28]

46. In describing its 2015 Focus, Ford states:

> Safety
>
> You don't have to pick and choose when it comes to safety. Focus is well equipped with an impressive list of safety features.[29]

GM

47. GM also heavily promotes the safety of its vehicles. As GM states in one of its promotional materials:

> GM's Commitment to Safety
>
> Quality and safety are at the top of the agenda at GM, as we work on technology improvements in crash avoidance and crashworthiness to augment the post-event benefits of OnStar, like advanced automatic crash notification.[30]

48. And in a recent press release, GM stated:

> GM Paves Way for Global Active Safety Development
>
> Thu, Oct 23 2014
>
> MILFORD, Mich. – General Motors today revealed that the development of one of the largest active automotive safety testing

[27] http://www.toyota.com/esq/safety/active-safety/advanced-driving-support-system.html (last accessed June 30, 2015).
[28] http://www.ford.com/cars/fusion/trim/s/safety/ (last accessed March 5, 2015).
[29] http://www.ford.com/cars/focus/trim/st/safety/ (last accessed March 5, 2015).
[30] http://www.gm.com/vision/quality_safety/gms_commitment_tosafety.html (last accessed June 30, 2015).

> areas in North America is nearly complete at its Milford Proving Ground campus.
>
> …
>
> The Active Safety Testing Area, or ASTA, will complement the Milford Proving Ground's vast test capabilities and increase GM's ability to bring the best new safety technologies to the customer.[31]

Defendants Collect and Transmit Vehicle Data in Violation of Privacy Rights

49. Without drivers ever knowing, Defendants also collect data from their vehicles and share the data with third parties.[32] While Defendants agreed to adopt voluntary privacy guidelines governing their collection and sharing of this data, the American Automobile Association and Senator Markey of Massachusetts stated that these measures are insufficient, as they do not provide drivers the right to control their own information and fail to allow drivers to withhold sensitive information from collection in the first instance.[33]

50. As detailed in Sen. Markey's report, Defendants collect large amounts of data on driving history and vehicle performance, and they transmit the data to third-party data centers without effectively securing the data.[34] Defendants only make drivers aware of such data collection in owners' manuals, online "privacy statements," and terms & conditions of specific feature activations—but drivers can't comprehensively opt out of all collection of data by Defendants, and in the limited situations where opting out is permitted, the driver must turn off a feature or cancel a service subscription.[35]

/./.

/./.

/./.

[31] http://www.gm.com/article.content_pages_news_us_en_2014_oct_1023-active-safety.~content~gmcom~home~vision~quality_safety.html (last accessed March 5, 2015).
[32] *See* Lucas Mearian, Once Your Car's Connected to The Internet, Who Guards Your Privacy? http://www.computerworld.com/article/2684298/once-your-cars-connected-to-the-internet-who-guards-your-privacy.html (last accessed June 30, 2015) (detailing practices of Defendants Ford and GM).
[33] *See* Kate Kaye, Ford, GM and Others to Adopt Data Privacy Rules, But AAA Says The Industry's Voluntary Guidelines Fall Short, http://adage.com/article/privacy-and-regulation/ford-gm-adopt-auto-data-privacy-rules/295859 (last accessed June 30, 2015) (detailing practices of Defendants Ford, GM, and Toyota).
[34] Markey Report at 8-11.
[35] *See* Markey Report at 12.

CLASS ALLEGATIONS

51. Plaintiffs bring this action on behalf of themselves and as a class action, pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following classes:

> All persons or entities who purchased or leased a GM Vehicle or Toyota Vehicle equipped with networked electronic or computerized components connected via a controller area network to an integrated cell phone or Class 1 or Class 2 master Bluetooth device in the State of California (the "California Class").
>
> All persons or entities who purchased or leased a Ford Vehicle equipped with networked electronic or computerized components connected via a controller area network to an integrated cell phone or Class 1 or Class 2 master Bluetooth device in the State of Oregon (the "Oregon Class").
>
> All persons or entities who purchased or leased a Ford Vehicle equipped with networked electronic or computerized components connected via a controller area network to an integrated cell phone or Class 1 or Class 2 master Bluetooth device in the State of Washington (the "Washington Class").
>
> (Collectively, the "Class," unless otherwise noted).

52. Excluded from the Class are Defendants and their subsidiaries and affiliates; all persons who make a timely election to be excluded from the Class; governmental entities; and the judge to whom this case is assigned and his/her immediate family.

53. Plaintiffs reserve the right to revise the Class definition based upon information learned through discovery.

54. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claim.

55. This action has been brought and may be properly maintained on behalf of each of the Classes proposed herein under Federal Rule of Civil Procedure 23.

56. Numerosity. Federal Rule of Civil Procedure 23(a)(1): The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiffs are informed and believe that there are not less than tens of thousands of members of the Class, the precise number of Class members is unknown to

Plaintiffs, but may be ascertained from Defendants' books and records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

57. Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3): This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

(a) Whether Defendants engaged in the conduct alleged herein;

(b) Whether Defendants designed, advertised, marketed, distributed, leased, sold, or otherwise placed Class Vehicles into the stream of commerce in the United States;

(c) Whether the Class Vehicles contain defects;

(d) Whether such defects can cause the Class Vehicles to malfunction;

(e) Whether Defendants knew about the defects and, if so, how long Defendants have known of the defects;

(f) Whether Defendants designed, manufactured, marketed, and distributed defective Class Vehicles;

(g) Whether Defendants' conduct violates consumer protection statutes, warranty laws, and other laws as asserted herein;

(h) Whether Defendants knew or reasonably should have known of the defects in the Class Vehicles before it sold or leased them to Class members;

(i) Whether Plaintiffs and the other Class members are entitled to equitable relief, including, but not limited to, restitution or injunctive relief; and

(j) Whether Plaintiffs and the other Class members are entitled to damages and other monetary relief and, if so, in what amount.

58. Typicality: Federal Rule of Civil Procedure 23(a)(3): Plaintiffs' claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' wrongful conduct as described above.

/././

59. Adequacy: Federal Rule of Civil Procedure 23(a)(4): Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Classes each respectively seeks to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs intend to prosecute this action vigorously. The Classes' interests will be fairly and adequately protected by Plaintiffs and their counsel.

60. Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2): Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Classes, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the Class as a whole.

61. Superiority: Federal Rule of Civil Procedure 23(b)(3): A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

/././

/././

/././

/././

/././

/././

VIOLATIONS ALLEGED

CLAIMS BROUGHT ON BEHALF OF THE CALIFORNIA CLASS

COUNT I

Violation Of California Unfair Competition Law

(Cal. Bus. & Prof. Code §§ 17200, et seq.)

62. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class against Defendants GM and Toyota.

63. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

64. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, et seq., proscribes acts of unfair competition, including "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising."

65. Defendants' conduct, as described herein, was and is in violation of the UCL. Defendants' conduct violates the UCL in at least the following ways:

(a) By knowingly and intentionally concealing from Plaintiffs and the other California Class members that the Class Vehicles suffer from a design defect while obtaining money from Plaintiffs;

(b) By refusing or otherwise failing to repair and/or replace defective electronic and computerized components in Class Vehicles;

(c) By violating other California laws, including Cal. Civ. Code §§ 1709, 1710, and 1750, et seq., Cal. Comm. Code § 2313, and (as set forth *infra* in Count VIII) Article I, Section 1 of the California Constitution.

66. Had Plaintiffs Cahen and Nisam known about the design defects that Defendants failed to disclose, they would not have purchased their Class Vehicles or would not have paid as much as they did to purchase them.

67. Plaintiffs seek to enjoin further unlawful, unfair, and/or fraudulent acts or practices by Defendants under Cal. Bus. & Prof. Code § 17200.

/./.

68. Plaintiffs request that this Court enter such orders or judgments as may be necessary to enjoin Defendants from continuing their unfair, unlawful, and/or deceptive practices and to restore to Plaintiffs and members of the Class any money Defendants acquired by unfair competition, including restitution and/or restitutionary disgorgement, as provided in Cal. Bus. & Prof. Code § 17203 and Cal. Civ. Code § 3345; and for such other relief set forth below.

COUNT II

Violation of California Consumers Legal Remedies Act

(Cal. Civ. Code §§ 1750, et seq.)

69. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class against Defendants GM and Toyota.

70. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

71. California's Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, et seq., proscribes "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer."

72. The Class Vehicles are "goods" as defined in Cal. Civ. Code § 1761(a).

73. Plaintiffs and the other California class members are "consumers" as defined in Cal. Civ. Code § 1761(d), and Plaintiffs, the other California class members, and Defendants are "persons" as defined in Cal. Civ. Code § 1761(c).

74. As alleged above, Defendants made numerous representations concerning the benefits and safety features of the Class Vehicles that were misleading.

75. In purchasing or leasing the Class Vehicles, Plaintiffs and the other California Class members were deceived by Defendants' failure to disclose that the Class Vehicles were equipped with defective electronic and computerized components.

76. Defendants' conduct, as described hereinabove, was and is in violation of the CLRA.

/./.

77. Defendants' conduct violates at least the following enumerated CLRA provisions:

(a) Cal. Civ. Code § 1770(a)(5): Representing that goods have characteristics, uses, and benefits which they do not have;

(b) Cal. Civ. Code § 1770(a)(7): Representing that goods are of a particular standard, quality, or grade, if they are of another;

(c) Cal. Civ. Code § 1770(a)(9): Advertising goods with intent not to sell them as advertised; and

(d) Cal. Civ. Code § 1770(a)(16): Representing that goods have been supplied in accordance with a previous representation when they have not.

78. Plaintiffs and the other California Class members have suffered injury in fact and actual damages resulting from Defendants' material omissions and misrepresentations because they paid an inflated purchase or lease price for the Class Vehicles.

79. Defendants knew, should have known, or were reckless in not knowing of the defective design and/or manufacture of the electronic and computerized components, and that they were not suitable for their intended use.

80. The facts concealed and omitted by Defendants to Plaintiffs and the other California Class members are material in that a reasonable consumer would have considered them to be important in deciding whether to purchase or lease the Class Vehicles or pay a lower price.

81. Had Plaintiffs Cahen and Nisam known about the design defects that Defendants failed to disclose, they would not have purchased their Class Vehicles or would not have paid as much as they did to purchase them.

82. Plaintiffs have provided Defendants with notice of their violations of the CLRA pursuant to Cal. Civ. Code § 1782(a). More than thirty (30) days have passed, and Defendants have failed to take any corrective action as required by Plaintiffs' notice or Cal. Civ. Code § 1782(b).

83. Plaintiffs' and the other California Class members' injuries were proximately caused by Defendants' fraudulent and deceptive business practices. Therefore, Plaintiffs and the

/././

other California Class members are entitled to equitable and monetary relief under the CLRA. Plaintiffs additionally seek monetary damages pursuant to the CLRA.

COUNT III

Violation of California False Advertising Law

(Cal. Bus. & Prof. Code §§ 17500, et seq.)

84. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class against Defendants GM and Toyota.

85. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

86. California Bus. & Prof. Code § 17500 states: "It is unlawful for any … corporation … with intent directly or indirectly to dispose of real or personal property … to induce the public to enter into any obligation relating thereto, to make or disseminate or cause to be made or disseminated … from this state before the public in any state, in any newspaper or other publication, or any advertising device, … or in any other manner or means whatever, including over the Internet, any statement … which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading."

87. Defendants have violated § 17500 because their omissions regarding the safety, reliability, and functionality of their Class Vehicles as set forth in this Complaint were material and likely to deceive a reasonable consumer.

88. Plaintiffs and the other Class members have suffered an injury in fact, including the loss of money or property, as a result of Defendants' unfair, unlawful, and/or deceptive practices. In purchasing or leasing their Class Vehicles, Plaintiffs and the other Class members relied on the omissions of Defendants with respect to the safety and reliability of the Class Vehicles..

89. Had Plaintiffs Cahen and Nisam known about the design defects that Defendants failed to disclose, they would not have purchased their Class Vehicles or would not have paid as much as they did to purchase them.

/././

90. All of the wrongful conduct alleged herein occurred, and continues to occur, in the conduct of Defendants' business. Defendants' wrongful conduct is part of a pattern or generalized course of conduct that is still perpetuated and repeated, both in the State of California and nationwide.

91. Plaintiffs, individually and on behalf of the other Class members, request that this Court enter such orders or judgments as may be necessary to enjoin Defendants from continuing their unfair, unlawful, and/or deceptive practices and to restore to Plaintiffs and the other Class members any money Defendants acquired by unfair competition, including restitution and/or restitutionary disgorgement, and for such other relief set forth below.

COUNT IV

Breach of Implied Warranty of Merchantability

(Cal. Com. Code § 2314)

92. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class against Defendants GM and Toyota.

93. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

94. Defendants are and were at all relevant times merchants with respect to motor vehicles under Cal. Com. Code § 2104.

95. A warranty that the Class Vehicles were in merchantable condition was implied by law in the instant transaction, pursuant to Cal. Com. Code § 2314.

96. These Class Vehicles, when sold and at all times thereafter, were not in merchantable condition and are not fit for the ordinary purpose for which cars are used. Specifically, the Class Vehicles are inherently defective in that there are defects in the electronic and computerized components; and they were not adequately designed, manufactured, and tested.

97. Defendants were provided notice of these issues by research studies, and by this Complaint, before or within a reasonable amount of time after the allegations of Class Vehicle defects became public.

/./.

98. Plaintiffs and the other Class members have had sufficient direct dealings with either Defendants or their agents (dealerships) to establish privity of contract between Plaintiffs and the other Class members. Notwithstanding this, privity is not required in this case because Plaintiffs and the other Class members are intended third-party beneficiaries of contracts between Defendants and their dealers; specifically, they are the intended beneficiaries of Defendants' implied warranties. The dealers were not intended to be the ultimate consumers of the Class Vehicles and have no rights under the warranty agreements provided with the Class Vehicles; the warranty agreements were designed for and intended to benefit the ultimate consumers only.

99. Finally, privity is also not required because Plaintiffs' and the other Class members' Class Vehicles are dangerous instrumentalities due to the aforementioned defects and nonconformities.

100. As a direct and proximate result of Defendants' breach of the warranties of merchantability, Plaintiffs and the other Class members have been damaged in an amount to be proven at trial.

COUNT V

Breach of Contract/Common Law Warranty

(Based on California Law)

101. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class against Defendants GM and Toyota.

102. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

103. To the extent Defendants' limited remedies are deemed not to be warranties under California's Commercial Code, Plaintiffs, individually and on behalf of the other Class members, plead in the alternative under common law warranty and contract law. Defendants limited the remedies available to Plaintiffs and the other Class members to repairs and adjustments needed to correct defects in materials or workmanship of any part supplied by Defendants and/or warranted the quality or nature of those services to Plaintiffs and the other Class members.

104. Defendants breached this warranty or contract obligation by failing to repair or

recall the Class Vehicles with faulty and defective electronic and computerized components, or to replace them.

105. As a direct and proximate result of Defendants' breach of contract or common law warranty, Plaintiffs and the other Class members have been damaged in an amount to be proven at trial, which shall include, but is not limited to, all compensatory damages, incidental and consequential damages, and other damages allowed by law.

COUNT VI

Fraud By Concealment

(Based on California Law)

106. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class against Defendants GM and Toyota.

107. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

108. As set forth above, Defendants concealed and/or suppressed material facts concerning the safety, quality, functionality, and reliability of their Class Vehicles.

109. Defendants had a duty to disclose these safety, quality, functionality, and reliability issues because they consistently marketed their Class Vehicles as safe and proclaimed that safety is one of Defendants' highest corporate priorities. Once Defendants made representations to the public about safety, quality, functionality, and reliability, Defendants were under a duty to disclose these omitted facts, because where one does speak one must speak the whole truth and not conceal any facts which materially qualify those facts stated. One who volunteers information must be truthful, and the telling of a half-truth calculated to deceive is fraud.

110. In addition, Defendants had a duty to disclose these omitted material facts because they were known and/or accessible only to Defendants which has superior knowledge and access to the facts, and Defendants knew they were not known to or reasonably discoverable by

/././

Plaintiffs and the other Class members. These omitted facts were material because they directly

impact the safety, quality, functionality, and reliability of the Class Vehicles.

111. Whether or not a vehicle is susceptible to hacking as a result of the defect alleged herein is a material safety concern. Defendants possessed exclusive knowledge of the defect rendering the Class Vehicles inherently more dangerous and unreliable than similar vehicles.

112. Defendants actively concealed and/or suppressed these material facts, in whole or in part, with the intent to induce Plaintiffs and the other Class members to purchase or lease Class Vehicles at a higher price for the Class Vehicles, which did not match the Class Vehicles' true value.

113. Defendants still have not made full and adequate disclosure and continues to defraud Plaintiffs and the other Class members.

114. Plaintiffs and the other Class members were unaware of these omitted material facts and would not have acted as they did if they had known of the concealed and/or suppressed facts. Plaintiffs' and the other Class members' actions were justified. Defendants were in exclusive control of the material facts and such facts were not known to the public, Plaintiffs, or the Class.

115. As a result of the concealment and/or suppression of the facts, Plaintiffs and the other Class members sustained damage.

116. Defendants' acts were done maliciously, oppressively, deliberately, with intent to defraud, and in reckless disregard of Plaintiffs' and the other Class members' rights and well-being to enrich Defendants. Defendants' conduct warrants an assessment of punitive damages in an amount sufficient to deter such conduct in the future, which amount is to be determined according to proof.

/././

/././

/././

/././

COUNT VII

Violation of Song-Beverly Consumer Warranty Act for

Breach of Implied Warranty of Merchantability

(Cal. Civ. Code §§ 1791.1 & 1792)

117. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class against Defendants GM and Toyota.

118. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

119. Plaintiffs and the other Class members who purchased or leased the Class Vehicles in California are "buyers" within the meaning of Cal. Civ. Code § 1791(b).

120. The Class Vehicles are "consumer goods" within the meaning of Cal. Civ. Code § 1791(a).

121. Defendants are "manufacturers" of the Class Vehicles within the meaning of Cal. Civ. Code § 1791(j).

122. Defendants impliedly warranted to Plaintiffs and the other Class members that their Class Vehicles were "merchantable" within the meaning of Cal. Civ. Code §§ 1791.1(a) & 1792, however, the Class Vehicles do not have the quality that a buyer would reasonably expect.

123. Cal. Civ. Code § 1791.1(a) states:

> "Implied warranty of merchantability" or "implied warranty that goods are merchantable" means that the consumer goods meet each of the following:
>
> (1) Pass without objection in the trade under the contract description.
>
> (2) Are fit for the ordinary purposes for which such goods are used.
>
> (3) Are adequately contained, packaged, and labeled.
>
> (4) Conform to the promises or affirmations of fact made on the container or label.

/./.

/./.

124. The Class Vehicles would not pass without objection in the automotive trade because of the defects in the Class Vehicles' electronic and computerized components that cause crucial functions of the Class Vehicles to be susceptible to hacking.

125. Because of the defects in the Class Vehicles' electronic and computerized components that cause crucial functions of the Class Vehicles to be susceptible to hacking, they are not safe to drive and thus not fit for ordinary purposes.

126. The Class Vehicles are not adequately labeled because the labeling fails to disclose the defects in the Class Vehicles' electronic and computerized components that cause crucial functions of the Class Vehicles to be susceptible to hacking.

127. Defendants breached the implied warranty of merchantability by manufacturing and selling Class Vehicles containing defects associated with the electronic and computerized components. Furthermore, these defects have caused Plaintiffs and the other Class members to not receive the benefit of their bargain and have caused Class Vehicles to depreciate in value.

128. As a direct and proximate result of Defendants' breach of the implied warranty of merchantability, Plaintiffs and the other Class members received goods whose dangerous and dysfunctional condition substantially impairs their value to Plaintiffs and the other Class members.

129. Plaintiffs and the other Class members have been damaged as a result of the diminished value of Defendants' products, the products' malfunctioning, and the nonuse of their Class Vehicles.

130. Pursuant to Cal. Civ. Code §§ 1791.1(d) & 1794, Plaintiffs and the other Class members are entitled to damages and other legal and equitable relief including, at their election, the purchase price of their Class Vehicles, or the overpayment or diminution in value of their Class Vehicles.

131. Pursuant to Cal. Civ. Code § 1794, Plaintiffs and the other Class members are entitled to costs and attorneys' fees.

/./.

COUNT VIII

Invasion of Privacy

(Cal. Const. Art. I, § 1)

132. Plaintiffs Cahen and Nisam bring this Count on behalf of the California Class

against Defendants GM and Toyota.

133. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

134. Plaintiffs are informed and believe, and thereupon allege, that in doing the things alleged herein, Defendants, without Plaintiffs' consent, violated their right to privacy established in Article I, Section 1 of the California Constitution.

135. Plaintiffs maintain a legally protected privacy interest in their personal data collected and transmitted to third parties by Defendants, including but not limited to the geographic location of their vehicles at various times.

136. Defendants knew, or should have known, that Plaintiffs had a reasonable expectation of privacy in their personal data, and that Defendants' collection and transmission to third parties of such data constituted a violation of Plaintiffs' constitutionally protected right to privacy.

137. Defendants' wrongful conduct as alleged herein, without regard to whether Defendants acted intentionally or with any other particular state of mind or scienter, renders Defendants liable to Plaintiffs for the wrongful violations of Plaintiffs' constitutionally protected right to privacy and for the damages caused thereby. In doing the acts as alleged herein, Defendants acted intentionally or with conscious disregard for Plaintiffs' right to privacy.

138. Plaintiffs have suffered damages as a result of Defendants' wrongful conduct, and Plaintiffs seek to enjoin Defendants from collecting and disseminating data obtained as a result of violating Plaintiffs' constitutionally protected right to privacy.

/./.

/./.

/./.

CLAIMS BROUGHT ON BEHALF OF THE OREGON CLASS

COUNT I

Violation of the Oregon Unlawful Trade Practices Act

(Or. Rev. Stat. §§ 646.605, et seq.)

139. Plaintiff Tompulis brings this Count on behalf of the Oregon Class against Defendant Ford.

140. Plaintiff realleges and incorporates by reference all paragraphs as though fully set forth herein.

141. The Oregon Unfair Trade Practices Act ("OUTPA") prohibits a person from, in the course of the person's business, doing any of the following: "(e) Represent[ing] that … goods … have … characteristics … uses, benefits, … or qualities that they do not have; (g) Represent[ing] that … goods … are of a particular standard [or] quality … if they are of another; and (i) Advertis[ing] … goods or services with intent not to provide them as advertised." OR. REV. STAT. § 646.608(1).

142. Defendant is a person within the meaning of OR. REV. STAT. § 646.605(4).

143. The Defective Vehicles at issue are "goods" obtained primarily for personal family or household purposes within the meaning of OR. REV. STAT. § 646.605(6).

144. In the course of Defendant's business, it willfully failed to disclose and actively concealed the dangerous risk of hacking and the lack of adequate fail-safe mechanisms in Defective Vehicles as described above. Accordingly, Defendant engaged in unlawful trade practices, including representing that Defective Vehicles have characteristics, uses, benefits, and qualities which they do not have; representing that Defective Vehicles are of a particular standard and quality when they are not; and advertising Defective Vehicles with the intent not to sell them as advertised. Defendant knew or should have known that its conduct violated the OUTPA.

145. As a result of these unlawful trade practices, Plaintiff has suffered ascertainable loss.

/././

146. Defendant engaged in a deceptive trade practice when it failed to disclose material

information concerning the vehicles that was known to Defendant at the time of the sale. Defendant deliberately withheld the information about the vehicles' susceptibility to hacking in order to ensure that consumers would purchase its vehicles and to induce the consumer to enter into a transaction.

147. The susceptibility of the vehicles to hacking and their lack of a fail-safe mechanism were material to Plaintiff and the Class. Had Plaintiff and the Class known that their vehicles had these serious safety defects, they would not have purchased their vehicles.

148. Plaintiff is entitled to recover the greater of actual damages or $200 pursuant to OR. REV. STAT. § 646.638(1). Plaintiff is also entitled to punitive damages because Defendant engaged in conduct amounting to a particularly aggravated, deliberate disregard of the rights of others.

149. Pursuant to OR. REV. STAT. § 646.638(2), Plaintiff will mail a copy of the complaint to Oregon's attorney general.

COUNT II

Breach of the Implied Warranty of Merchantability

(Or. Rev. Stat. § 72.3140)

150. Plaintiff Tompulis brings this Count on behalf of the Oregon Class against Defendant Ford.

151. Plaintiff realleges and incorporates by reference all paragraphs as though fully set forth herein.

152. Defendant is and was at all relevant times a merchant with respect to motor vehicles.

153. A warranty that the Class Vehicles were in merchantable condition is implied by law in the instant transactions.

154. These Class Vehicles, when sold and at all times thereafter, were not in merchantable condition and are not fit for the ordinary purpose for which cars are used.

/././

Defendant was provided notice of these issues by numerous complaints filed against it, including

the instant Complaint, and by other means.

155. As a direct and proximate result of Defendant's breach of the warranties of merchantability, Plaintiff and the Class have been damaged in an amount to be proven at trial.

COUNT III

Fraudulent Concealment

(Based on Oregon Law)

156. Plaintiff Tompulis brings this Count on behalf of the Oregon Class against Defendant Ford.

157. Plaintiff realleges and incorporates by reference all paragraphs as though fully set forth herein.

158. Defendant intentionally concealed the above-described material safety and functionality information, or acted with reckless disregard for the truth, and denied Plaintiff and the other Class members' information that is highly relevant to their purchasing decision.

159. Defendant further affirmatively misrepresented to Plaintiff in advertising and other forms of communication, including standard and uniform material provided with each car, that the Class Vehicles it was selling were new, had no significant defects, and would perform and operate properly when driven in normal usage.

160. Defendant knew these representations were false when made.

161. The Class Vehicles purchased or leased by Plaintiff and the other Class members were, in fact, defective, unsafe, and unreliable because the Class Vehicles contained faulty and defective electronic and computerized components, as alleged herein.

162. Defendant had a duty to disclose that these Class Vehicles were defective, unsafe, and unreliable in that certain crucial safety functions of the Class Vehicles would be rendered inoperative due to faulty and defective electronic and computerized components, because Plaintiff and the other Class members relied on Defendant's material representations that the Class Vehicles they were purchasing were safe and free from defects.

/././

163. The aforementioned representations were material because they were facts that

would typically be relied on by a person purchasing or leasing a new motor vehicle. Defendant knew or recklessly disregarded that its representations were false because it knew the Class Vehicles were susceptible to hacking. Defendant intentionally made the false statements in order to sell Class Vehicles.

164. Plaintiff and the other Class members relied on Defendant's reputation – along with Defendant's failure to disclose the faulty and defective nature of the electronic and computerized components and Defendant's affirmative assurances that its Class Vehicles were safe and reliable, and other similar false statements – in purchasing or leasing Defendant's Class Vehicles.

165. As a result of their reliance, Plaintiff and the other Class members have been injured in an amount to be proven at trial, including, but not limited to, their lost benefit of the bargain and overpayment at the time of purchase or lease and/or the diminished value of their Class Vehicles.

166. Defendant's conduct was knowing, intentional, with malice, demonstrated a complete lack of care, and was in reckless disregard for the rights of Plaintiff and the other Class members.

167. Plaintiff and the other Class members are therefore entitled to an award of punitive damages.

CLAIMS BROUGHT ON BEHALF OF THE WASHINGTON CLASS

COUNT I

Violation of the Consumer Protection Act

(Rev. Code Wash. Ann. §§ 19.86.010, et seq.)

168. Plaintiffs Gibbs and Langdon bring this Count on behalf of the Washington Class against Defendant Ford.

169. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

/././

170. The conduct of Defendant as set forth herein constitutes unfair or deceptive acts or

practices, including, but not limited to, Defendant's manufacture and sale of vehicles with faulty and defective electronic and computerized components rendering Class Vehicles susceptible to hacking, which Defendant failed to adequately investigate, disclose and remedy, and its misrepresentations and omissions regarding the safety and reliability of its vehicles.

171. Defendant's actions as set forth above occurred in the conduct of trade or commerce.

172. Defendant's actions impact the public interest because Plaintiffs were injured in exactly the same way as millions of others purchasing and/or leasing Defendant's vehicles as a result of Defendant's generalized course of deception. All of the wrongful conduct alleged herein occurred, and continues to occur, in the conduct of Defendant's business.

173. Plaintiffs and the Class were injured as a result of Defendant's conduct. Plaintiffs overpaid for their Defective Vehicles and did not receive the benefit of their bargain, and their vehicles have suffered a diminution in value.

174. Defendant's conduct proximately caused the injuries to Plaintiffs and the Class.

175. Defendant is liable to Plaintiffs and the Class for damages in amounts to be proven at trial, including attorneys' fees, costs, and treble damages.

176. Pursuant to WASH. REV. CODE ANN. § 19.86.095, Plaintiffs will serve the Washington Attorney General with a copy of this complaint as Plaintiffs seek injunctive relief.

COUNT II

Breach of the Implied Warranty of Merchantability

(Rev. Code Wash. § 62A.2-614)

177. Plaintiffs Gibbs and Langdon bring this Count on behalf of the Washington Class against Defendant Ford.

178. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

179. Defendant is and was at all relevant times a merchant with respect to motor vehicles.

180. A warranty that the Class Vehicles were in merchantable condition is implied by

law in the instant transactions.

181. These Class Vehicles, when sold and at all times thereafter, were not in merchantable condition and are not fit for the ordinary purpose for which cars are used. Defendant was provided notice of these issues by numerous complaints filed against it, including the instant Complaint, and by other means.

182. Privity is not required in this case because Plaintiffs and the Class are intended third-party beneficiaries of contracts between Defendant and its dealers; specifically, they are the intended beneficiaries of Defendant's implied warranties. The dealers were not intended to be the ultimate consumers of the Defective Vehicles and have no rights under the warranty agreements provided with the Defective Vehicles; the warranty agreements were designed for and intended to benefit the ultimate consumers only.

183. As a direct and proximate result of Defendant's breach of the warranties of merchantability, Plaintiffs and the Class have been damaged in an amount to be proven at trial.

COUNT III

Breach of Contract/Common Law Warranty

(Based on Washington Law)

184. Plaintiffs Gibbs and Langdon bring this Count on behalf of the Washington Class against Defendant Ford.

185. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

186. To the extent Defendant's limited remedies are deemed not to be warranties under Washington's Commercial Code, Plaintiffs, individually and on behalf of the other Class members, plead in the alternative under common law warranty and contract law. Defendant limited the remedies available to Plaintiffs and the other Class members to repairs and adjustments needed to correct defects in materials or workmanship of any part supplied by Defendant, and/or warranted the quality or nature of those services to Plaintiffs and the other Class members.

187. Defendant breached this warranty or contract obligation by failing to repair or

recall the Class Vehicles, or to replace them.

188. As a direct and proximate result of Defendant's breach of contract or common law warranty, Plaintiffs and the other Class members have been damaged in an amount to be proven at trial, which shall include, but is not limited to, all compensatory damages, incidental and consequential damages, and other damages allowed by law.

COUNT IV

Fraudulent Concealment

(Based on Washington Law)

189. Plaintiffs Gibbs and Langdon bring this Count on behalf of the Washington Class against Defendant Ford.

190. Plaintiffs reallege and incorporate by reference all paragraphs as though fully set forth herein.

191. Defendant intentionally concealed the above-described material safety and functionality information, or acted with reckless disregard for the truth, and denied Plaintiffs and the other Class members' information that is highly relevant to their purchasing decision.

192. Defendant further affirmatively misrepresented to Plaintiffs in advertising and other forms of communication, including standard and uniform material provided with each car, that the Class Vehicles they was selling were new, had no significant defects, and would perform and operate properly when driven in normal usage.

193. Defendant knew these representations were false when made.

194. The Class Vehicles purchased or leased by Plaintiffs and the other Class members were, in fact, defective, unsafe, and unreliable because the Class Vehicles contained faulty and defective electronic and computerized components, as alleged herein.

195. Defendant had a duty to disclose that these Class Vehicles were defective, unsafe, and unreliable in that certain crucial safety functions of the Class Vehicles would be rendered inoperative due to faulty and defective electronic and computerized components, because Plaintiffs and the other Class members relied on Defendant's material representations that the Class Vehicles they were purchasing were safe and free from defects.

196. The aforementioned representations were material because they were facts that would typically be relied on by a person purchasing or leasing a new motor vehicle. Defendant knew or recklessly disregarded that its representations were false because it knew the Class Vehicles were susceptible to hacking. Defendant intentionally made the false statements in order to sell Class Vehicles.

197. Plaintiffs and the other Class members relied on Defendant's reputation – along with Defendant's failure to disclose the faulty and defective nature of the Class Vehicles and Defendant's affirmative assurances that its Class Vehicles were safe and reliable, and other similar false statements – in purchasing or leasing Defendant's Class Vehicles.

198. As a result of their reliance, Plaintiffs and the other Class members have been injured in an amount to be proven at trial, including, but not limited to, their lost benefit of the bargain and overpayment at the time of purchase or lease and/or the diminished value of their Class Vehicles.

199. Defendant's conduct was knowing, intentional, with malice, demonstrated a complete lack of care, and was in reckless disregard for the rights of Plaintiffs and the other Class members.

200. Plaintiffs and the other Class members are therefore entitled to an award of punitive damages.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the California, Oregon, and Washington Classes, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. Certification of the proposed California, Oregon and Washington Classes, including appointment of Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;

2. An order temporarily and permanently enjoining Defendants from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

3. Injunctive relief in the form of a recall or free replacement program;

4. Repair of the class vehicles to provide adequate security to prevent hacking, such as the addition of Trusted Platform Modules (TPM) or the equivalent;

5. Costs, restitution, damages, including punitive damages, and disgorgement in an amount to be determined at trial;

6. An order requiring Defendants to pay both pre- and post-judgment interest on any amounts awarded;

7. An award of costs and attorneys' fees; and

8. Such other or further relief as may be appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial for all claims so triable.

DATED: July 1, 2015 STANLEY LAW GROUP

/s/ Matthew J. Zevin

MATTHEW J. ZEVIN
10021 Willow Creek Road, Suite 200
San Diego, CA 92131
Telephone: (619) 235-5306
Facsimile: (815) 377-8419
e-mail: mzevin@aol.com

STANLEY LAW GROUP
MARC R. STANLEY, Texas SBN: 19046500
MARTIN WOODWARD, Texas SBN: 00797693
6116 North Central Expressway, Suite 1500
Dallas, TX 75206
Telephone: (214) 443-4300
Facsimile: (214) 443-0358
e-mail: marcstanley@mac.com
mwoodward@stanleylawgroup.com

Donald H. Slavik (application for Pro Hac Vice forthcoming)
SLAVIK LAW FIRM, LLC
2834 Blackhawk Court
Steamboat Springs, Colorado 80487-2018
Telephone: (970) 457-1011
dslavik@slavik.us

Attorneys for Plaintiffs

AFFIDAVIT OF VENUE BY PLAINTIFF HELENE CAHEN

I, HELENE CAHEN, hereby declare that:

1. I have personal knowledge of the facts stated herein. If called upon, I could and would competently testify to the facts contained in this Affidavit.

2. I am a Plaintiff in the above-entitled action.

3. My Complaint filed in this matter contains causes of action for violations of multiple California statutes against Toyota Motor Corporation ("TMC") and Toyota Motor Sales, U.S.A., Inc. ("TMS") (together, "Toyota"). TMC is a Japanese corporation doing business nationwide, including California, and is the parent of TMS. TMS is a California corporation that does business nationwide, including in Marin County. These causes of action arise out of my purchase of a 2008 Lexus RX 400 H, which was falsely marketed as safe.

4. I purchased the Lexus RX 400 H in Marin County, California.

I declare under penalty of perjury under the laws of the State of California that the foregoing affidavit is true and correct, and was executed by me in the City of Oakland, California on March 6, 2015.

H. Cahen

HELENE CAHEN

AFFIDAVIT OF VENUE BY PLAINTIFF MERRILL NISAM

I, MERRILL NISAM, hereby declare that:

1. I have personal knowledge of the facts stated herein. If called upon, I could and would competently testify to the facts contained in this Affidavit.

2. I am a Plaintiff in the above-entitled action.

3. My Complaint filed in this matter contains causes of action for violations of multiple California statutes against General Motors LLC, a Delaware limited liability company doing business nationwide, including in Marin County. These causes of action arise out of my purchase of a 2013 Chevrolet Volt, which was falsely marketed as safe.

4. I purchased the Chevrolet Volt in Marin County, California.

I declare under penalty of perjury under the laws of the State of California that the foregoing affidavit is true and correct, and was executed by me in the City of Mill Valley California on March 6 2015.

Merrill Nisam
MERRILL NISAM

Tracking & Hacking:

Security & Privacy Gaps Put American Drivers at Risk

ED MARKEY
United States Senator for Massachusetts

FEBRUARY 2015
WWW.MARKEY.SENATE.GOV

EXHIBIT 1

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

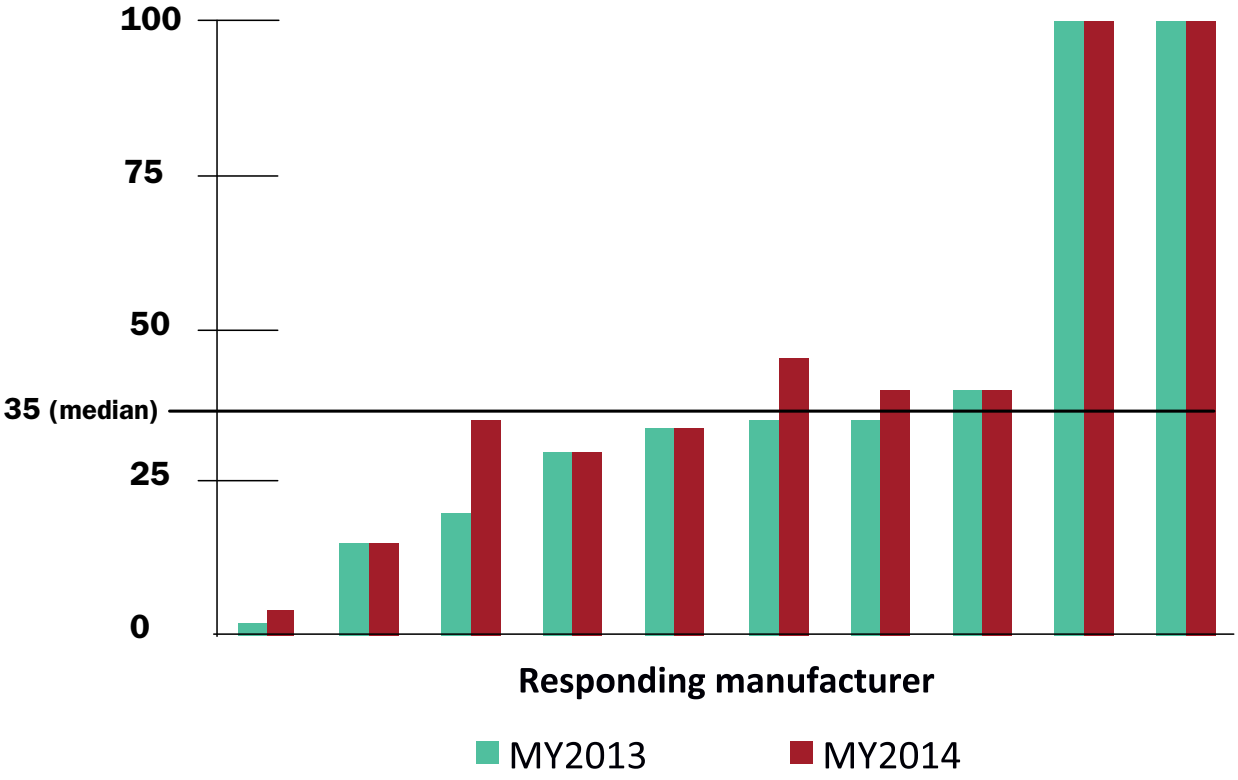


EXHIBIT 1

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.

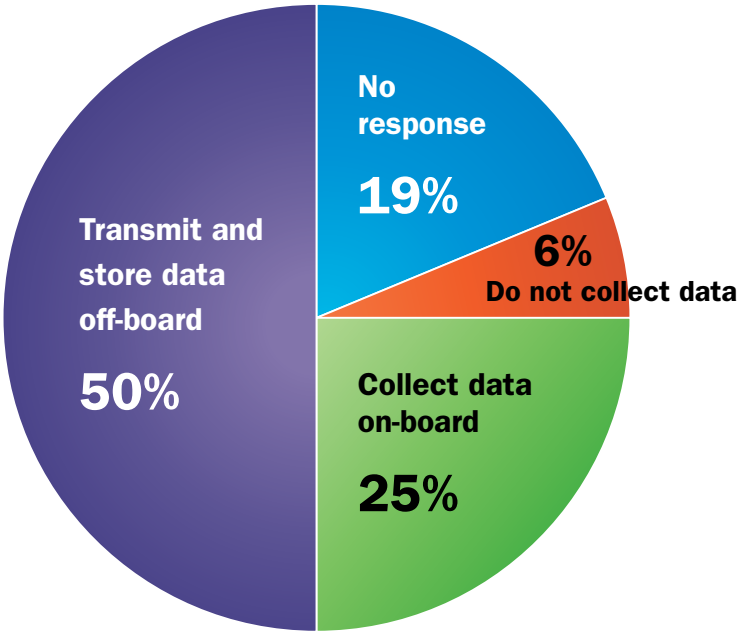
Finding #6: A majority of automakers offer technologies that collect and wirelessly transmit driving history data to data centers, including third-party data centers, and most do not describe effective means to secure the data.

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.