EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:

COMMERCE, SCIENCE, AND TRANSPORTATION
SMALL BUSINESS AND ENTREPRENEURSHIP
FOREIGN RELATIONS

CHAIRMAN:

SUBCOMMITTEE ON INTERNATIONAL DEVELOPMENT AND FOREIGN ASSISTANCE, ECONOMIC AFFAIRS, INTERNATIONAL ENVIRONMENTAL PROTECTION, AND PEACE CORPS

U.S. SENATE CLIMATE CHANGE CLEARING HOUSE

United States Senate

SUITE SR-218
RUSSELL BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

THOMAS P. O'NEILL, JR. FEDERAL BUILDING
10 CAUSEWAY STREET, SUITE 559
BOSTON, MA 02222
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01101
413-785-4610

December 2, 2013

Mr. Ludwig Willisch
Chief Executive Officer
BMW North America
300 Chestnut Ridge Road
Woodcliff Lake, NJ 07677

Dear Mr. Willisch,

I write to request information regarding your company's protections against the threat of cyber-attacks or unwarranted invasions of privacy related to the integration of wireless, navigation, and other technologies into and with automobiles.

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. My concerns are based on two recent developments that highlight potential threats to both automobile security and to consumer privacy.

In a recent study that was funded by the Defense Advanced Research Projects Agency (DARPA), Charlie Miller and Chris Valasek demonstrated their ability to directly connect to a vehicle's computer systems, send commands to different ECUs through the CAN, and thereby control the engine, brakes, steering and other critical vehicle components.[1] They were able to cause cars to suddenly accelerate, turn, and kill the brakes[2].

[1] "Adventures in Automotive Networks and Control Units," Dr. Charlie Miller and Chris Valasek, http://illmatics.com/car_hacking.pdf
[2] http://www.npr.org/blogs/alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New-Doors-To-Smarter-Thieves

Before the researchers went public with their findings, they shared the results with Ford and Toyota 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.[3]

A second, related area of concern to me 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.[4] This concern was highlighted when OnStar proposed to sell information about vehicles and their drivers, including a car's location and speed, odometer reading, driver seat-belt use, and air-bag deployment.[5] It was also revealed that Tesla Motors recorded data during a test drive of one of its vehicles by a reporter, including data related to the driver's location, energy usage, speed, temperature and other control settings, to rebut the reporter's unfavorable review of his driving experience.[6] 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[7] 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.

As vehicles 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, I request that you respond to the following questions by January 3, 2014:

---

[3] 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

[4] "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

[5] "Changes to OnStar's Privacy Terms Rile Some Users", John R. Quain, The New York Times http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users/

[6] 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

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

Questions related to your company's automotive security efforts. Please note that it is not my intent to publicly disclose *company-specific* security-related information that could increase a threat to automobile owners.

1) What percentage of your company's vehicle models that were available for sale in the United States in MY 2013 do not have *any* wireless entry points? What is the estimated percentage for your MY 2014 vehicles?

2) Please specifically describe the manner in which your company assesses whether there are vulnerabilities related to the technologies it purchases from other manufacturers as well as the wireless entry points of its vehicles to ensure that malicious code or other infiltrations cannot occur. Please include but not limit your response to the manner in which your company assesses any vulnerabilities associated with its a) tire pressure monitoring systems, b) bluetooth or other wireless communications technologies, including WIFI, c) Onstar or other navigation system technologies, d) technologies used to integrate the driver's smart phone or other mobile devices with the vehicle, e) web browsers or other applications, f) the ECU's themselves, since they are generally purchased from other manufacturers, g) vehicle-to-vehicle communications technologies and h) any other wireless entry points included on any of your models.

3) Does any of the testing described above include the use of independent third parties who are contracted by your company to attempt to infiltrate your vehicles' wireless entry points in order to identify (and, as needed, recommend a remedy) any such vulnerabilities? If so, please describe all such efforts, including a) how many of your vehicle models were subjected to such third party testing, b) the results of such testing, and c) your plans for such testing going forward.

4) Do any of your vehicles include technology that can monitor your vehicles' CAN buses in order to detect anomalous activity that could indicate that a cyber-attack or inadvertent introduction of malicious code has occurred? If so, please specify both the type of technology utilized as well as the percentage of your company's models that utilize it. If not, then how would you be alerted to the possibility that a cyber-attack or inadvertent introduction of malicious code has occurred?

5) Do any of your vehicles include technology that monitors your vehicles' wireless entry points in order to detect anomalous activity that could indicate that an unauthorized intrusion or inadvertent introduction of malicious code has occurred? If so, please specify both the type of technology utilized, the percentage of your company's models that utilize it, and how your company ensures that the data collected is uncompromised and accurate. If not, then how would you be alerted to the possibility that an unauthorized intrusion or inadvertent introduction of a computer virus has occurred?

6) Please describe the manner in which your company would respond to reports or detection of an unauthorized intrusion, remote attack, or inadvertent introduction of malicious code

to a wireless entry point of a vehicle or vehicles. Are there specific measures that could be taken to safely and remotely shut down the vehicle, notify the vehicle's owner and law enforcement authorities, and ensure that any damage is not propagated to other vehicles? If so, please describe them.

7) For *each* of the past five years, please list and fully describe all instances in which a) your company was made aware of an alleged intentional effort to infiltrate a wireless entry point of one of your company's vehicles or b) your company was made aware of the inadvertent introduction of malicious code into one of your company's vehicles through the driver's cell phone, navigation system or other technology (including ECUs) integrated into the vehicle. For each instance, please indicate the make and model of the vehicle, the date on which the instance occurred, any personal injury or vehicular or property damage alleged to have occurred as a result of the instance, whether the instance was reported to federal or local authorities (and if so, to what entity was the report made), and what changes, if any, were made to your vehicles to protect against similar vulnerabilities from being exploited in the future.

8) Many safety recalls today are conducted via the download of software fixes or updates. For each of the past five years, please provide the total number of a) safety recalls and b) service campaigns your company has issued in the U.S., and how many of each of these involved the download of software fixes or updates. What security measures are in place to ensure that these downloads are only available to your company's franchised dealers or authorized service facilities? What security measures are in place to ensure that malware cannot be inadvertently or deliberately introduced by those downloading the software fixes or updates?

Questions related to your company's privacy efforts. Please do not include in your responses information related to data that is stored on vehicle 'event data recorders' as that term is defined by the National Highway Traffic Safety Administration[8].

1) What types of navigation technology or other technologies are deployed (or have the option to be deployed if the consumer purchases them) in your company's vehicles that have the ability to collect driving history information? Please describe these technologies. What percentage of the automobiles sold in the United States by your company in MY 2013 included navigation technology or other technologies that can provide location information? What is the estimated percentage for your MY 2014 vehicles?

2) What types of driving history information can be collected by these technologies (including but not limited to geo-location, tire-pressure monitoring data, time of day, speed, distance traveled, seat belt use)?

3) Does your company provide these technologies and/or services directly or does it contract with another entity to provide these technologies and/or services? If yes, please list the entities with which your company contracts.

4) Is this driving history information recorded and stored (other than on an "event data recorder" as defined by the National Highway Traffic Safety Administration[9])?

   a. If the information is recorded and stored, is the information recorded and stored by your company and/or the company providing the navigation or similar technology/services?

   b. If the information is recorded and stored, for how long is the information stored?

   c. If the information is recorded and stored, where is the information stored (i.e., vehicle's computer systems, company's computer systems, cloud, etc.)?

   d. If the information is recorded and stored, how is your company and/or the company providing the navigation or similar technologies/services able to retrieve the information (i.e., wirelessly, physically accessing the car, etc.)?

   e. If the information is recorded and stored, how is that information secured against those seeking to obtain unauthorized access to it?

   f. If any recording or data storage technologies related to a vehicle as described above are installed either by your company or the company providing the navigation or similar technology, are consumers made aware of these activities before they purchase, lease or rent these vehicles? If yes, how are they made aware? If not, why not?

   g. If the information is recorded and stored, do consumers have the ability to request access to or deletion of this information? If not, why not? If yes, please explain how consumers can make these requests, and how consumers are made aware both of the existence of this information as well as of their ability to request access to or deletion of it.

   h. If the information is recorded and stored, can a consumer disable any such data recording of his or her driving history, and if so how? If not, why not? If a customer does not have a choice of whether to disable navigation services, is information still gathered about the consumer? If yes, what information is collected?

---

9 http://www.nhtsa.gov/Research/Event+Data+Recorder+(EDR)/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site

i. For what purposes does your company use this information (i.e. marketing, safety, research)?

5) Does your company sell or otherwise provide this information to third parties? If yes, does your company anonymize the information (i.e., disassociate individual records with customer identity, license plate, car serial number, etc.)? If the information has never been provided to third parties, is that because your company has a policy that restricts the provision of such information to third parties?

6) Can any such recording or data storage capabilities also be installed: a) by an automobile dealer, or b) by an automobile rental company? Please specifically describe all efforts to install such technologies on your company's vehicles about which you are aware.

7) For each of the past five years please indicate whether your company received a request for data related to the driving history of a particular driver or drivers?

   a. Within that total, please list the number of requests that have come from each requester (i.e., local law enforcement, federal agency, debt collector, insurance company, private detective, etc.).

   b. Please describe the reasons for these information requests.

   c. Please describe the types of information requested.

   d. Please describe the standard your company used to determine whether the request would be fulfilled (and whether different standards are required to fulfill requests for different types of stored information or requests from different types of requestors).

   e. What percentage of these information requests were fulfilled by your company?

   f. Was compensation requested to provide this information? If yes, how much was collected in each year?

8) What percentage of your company's models available for sale in the United States in MY 2013 include technology (or the option to purchase services/products that include the technology) that can enable the remote shut down of the vehicle? What is the estimated percentage for your MY 2014 vehicles?

9) Can technologies that enable the remote shut-down of the vehicle be installed: a) by an automobile dealer, or b) by an automobile rental company? Please specifically describe all efforts to install such technologies about which you are aware.

10) If technologies that can enable the remote shut down of a vehicle are installed either by your company or the company providing the navigation or similar technology, are consumers made aware of this capability before they purchase, lease or rent these vehicles? Can a consumer prevent the remote shut down of his or her vehicle, and if so how?

Thank you for your attention to this important matter. Please provide responses to these questions no later than January 3, 2014. If you have any questions, please have a member of your staff contact Michal Freedhoff or Joseph Wender at 202-224-2742.

Sincerely,

Edward J. Markey

Edward J. Markey
United States Senator