Privacy & In-Vehicle Telematics: The Road Ahead

Hilary M. Cain
Director of Technology and Innovation Policy
Toyota Motor North America, Inc.
Telematics 101

Tele-what?

The integration of telecommunications and computing technology in the vehicle, generally to provide services and information to drivers.
Emergency Assistance

- **Emergency Assistance**: A helping hand when you need it.
- **Stolen Vehicle Locator**: Your partner against crime.
- **Roadside Assistance**: Let us get you moving again.
- **Automatic Collision Notification**: We can call for help if you can’t.

*TOYOTA*
Vehicle Health and Maintenance

- Vehicle health reports
- Maintenance alerts
- Diagnostic Trouble Code notifications
- Recall advisories
What Data Is Currently Being Collected?

Not much.

Data for subscription- or registration-based services

- Vehicle location data
- Vehicle health details
- Vehicle status information
Data Sharing

Enables subscription- or registration-based service requested by the customer.

**May be shared with:**
- Telematics service providers
- Emergency personnel, roadside assistance providers
- 3rd-party app providers
Anonymized, aggregated data may also be shared with 3rd parties in limited circumstances:

- Traffic service providers to support real-time traffic data
- Regulatory agencies, non-profit organizations .... for research

Automakers may be forced to share data to comply with legal or court orders.
Unanswered Questions

Is **all** telematics data sensitive information?

- Location data
- Air bag deployment data
- Diagnostic Trouble Codes
- Status of powered doors and windows
Notice and Choice: How Do They Apply?

Distracted driving limits the ability to do real-time notice and choice

Real-time notice and choice may not always be possible

Contextual considerations

How long is it appropriate for data surrounding a specific request for service to be stored?
Growing Regulatory Interest
“All 10 selected companies have taken steps consistent with some, but not all, industry-recommended privacy practices. In addition, the companies’ privacy practices were, in certain instances, unclear, which could make it difficult for consumers to understand the privacy risks that may exist.”

“Sen. Franken said that the findings demonstrate that while companies providing in-car location services have taken concrete steps to protect their customers’ privacy, more work needs to be done to ensure privacy protections for in-car navigation systems and devices….He also said that this report has encouraged him to reintroduce his location privacy legislation sometime this year.”

- Senator Franken’s Press Release (January 6, 2014)
Growing Lawmaker Interest

“I write to request information regarding your company’s protections against the threat of cyber-attacks or unwarranted invasions of privacy…”

December 2, 2013

Mr. Shigeki Terashi
Chief Operating Officer
Toyota North America
19001 South Western Ave
Torrance, CA 90501

Dear Mr. Terashi,

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 Network or LIN). Vehicle functionality, safety, and security 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 vehicle’s operation. My concerns are based on recent developments that highlight potential threats to both automobile security and consumer privacy.

In a recent study that was funded by the Defense Advanced Research Projects Agency (DARPA), Dr. Charlie Miller and Chris Valasek demonstrated their ability to directly connect to a vehicle’s computer system, 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 control the vehicle to suddenly accelerate, turn, and kill the brakes.

1“Adversarial in Automotive Networks and Control Units,” Dr. Charlie Miller and Chris Valasek,
http://www.crowdsource hacking.pdf

15
Growing Lawmaker Interest

SCHUMER REVEALS: CARS ARE COLLECTING REAMS OF DATA ON DRIVERS, ALLOWING CAR, GPS AND AUTO DEVICE COMPANIES TO KEEP TABS ON YOUR EVERY MOVEMENT AND SELL DATA TO HIGHEST BIDDER – CALLS ON FTC AND NHTSA TO ESTABLISH CLEAR, ROBUST GUIDELINES TO ENSURE PRIVACY BEHIND THE WHEEL

-FEBRUARY 24, 2014