Connecting the Car: Managing the Risks of Cybersecurity and Privacy

7.23.2015

Technological innovation and the world of connectivity are moving rapidly, leaving legislators and proposed legislation far behind. The "Internet of Things"—from smart refrigerators to gadgets that sit aside our foreheads and zap us to be restful or alert—includes our increasingly "smart" cars. Automobiles are now mobile devices capable of transmitting and receiving data, whether running or not. Whether a component manufacturer to an EOM or a digital provider streaming content into the vehicle, you are now on notice: new concerns surround vehicle hacking that may put drivers—and vehicle suppliers—at risk.

Hacked! Jeep Falls Victim to a Wireless Cyberattack

Once considered a remote threat, hackers have demonstrated that cars can be attacked through new technology that promises to keep us connected. Similar to the 60 Minutes piece, WIRED Magazine highlighted an incident where two security researchers disabled a Jeep Cherokee by hacking into the car. Rather than using a direct "wired" connection, they used the wireless UConnect system. Because the UConnect system uses Sprint's cellular network for connectivity, the researchers could remotely locate a target vehicle by scanning for devices in a certain spectrum. The researchers issued commands through the vehicle's entertainment system that impacted dashboard functions, steering, brakes and transmission. In this way, they controlled the radio, blasted the air conditioning to full bore, operated the windshield wipers, and disabled the vehicle's accelerator, slowing it to a crawl. All this was controlled from a laptop 10 miles away.

Cars, Cybersecurity and Data Privacy: The Congressional Response

In a coincidental stroke of timeliness, on the same day the Jeep hack broke (July 21, 2015) Senators Richard Blumenthal, D-Conn., and Ed Markey, D-Mass., unveiled the Security and Privacy in Your

Related Services

Connected Car and Autonomous Vehicles

Cybersecurity and Privacy Specialty Team

Car (SPY Car Act). This Act would direct both the National Highway Traffic Safety Administration ("NHTSA") and the Federal Trade Commission ("FTC") to set industry-wide benchmarks to protect consumers from security and privacy threats to their motor vehicles. Noting that "[d]rivers shouldn't have to choose between being connected and being protected," Senator Markey emphasized the need for minimum standards with clear rules.

Accordingly, the SPY Car Act would establish:

- Cybersecurity standards requiring all entry points to the electronic systems to be equipped with reasonable measures to protect against hacking attacks.
- Continuous evaluation of security vulnerabilities that incorporates best practices including penetration testing.
- A response requirement where manufacturers must ensure that vehicles are equipped with the capability to immediately detect, report and stop attempts to intercept driving data or control the vehicle.
- Privacy and security controls over data to reasonably prevent unauthorized access for data stored in the vehicle at rest, data is in transit and any offboard storage or use of data.
- A protocol to allow vehicle owners/lessees to terminate the collection and retention of driving data without loss of navigation tools or other features.
- An express consent regime in which the owner/lessee would have to consent to any data collection in the vehicle not linked to accident investigation, emissions checks, crash avoidance or authorized regulatory compliance programs.
- Penalties up to $5,000 for each violation of the Act.

Surviving in the Black Hat World: Protecting the Company in Today's Cyber-Landscape

In response to the WIRED story on the Jeep, Chrysler quickly created a software update to address the vulnerability in the Uconnect system. Owners/lessees may now download the update onto a USB drive and plug it into their vehicle or take the vehicle to a dealership for a free software upgrade. While many consumer electronics companies are accustomed to pushing updates, this is relatively new territory for OEMs and the supply base. Suppliers, technology licensors and digital content providers should be aware of and prepared to address the following potential issues. What are the main takeaways? ***Security by design, privacy by design and continuous monitoring for threats.***

1. Obligations will increase

Software demands constant monitoring and updating. Given the extended time drivers keep automobiles and consumer's expectations for updated software, OEMs and suppliers will need to address the concerns of maintaining a longer-term relationship with the end user relating to electronic component and software performance. Indeed, federal regulation such as the proposed SPY Car Act may require such activities. Software vulnerabilities, cyber-threats and integration concerns will no doubt lead to safety campaigns, recalls and increased warranty actions. This will be

coupled with additional software maintenance obligations and intellectual property rights discussions that will impact content providers, software companies and electronic component manufacturers.

2. Accountability will linger

Suppliers, technology licensors and content providers will need to respond to safety issues and warranty concerns with ongoing programming changes that may well exceed the typical life of a standard warranty. Warranty issues become much more complex for software and software-dependent parts. For example, is there an ongoing obligation to protect against vulnerabilities? Who is responsible for preparing and providing any update? How long does the responsibility last? These and a myriad of other issues must be carefully addressed in the contract formation stage.

3. Ownership rights will take center-stage

Even though the SPY Car Act addresses issues surrounding the collection and storage of data in the vehicle, it does not clearly attribute ownership of the data generated by an automobile and its driver. Data ownership and its use and access are highly prized. Insurers, technology companies, content providers, state governments, suppliers and vehicle manufacturers all want in on the trove. As the battle for data ownership and control unfolds, companies must take the appropriate steps to secure rights while at the same time addressing privacy and security risks.

4. Contracts addressing evolving and innovative technologies will become more complex

Suppliers, technology licensors and content providers may be able to mitigate some of these issues through initial negotiations, addressing the risks in the terms and conditions of their agreements. During negotiations, it will be critical to address the cost of engineering security and privacy by design —issues not familiar to most automotive engineers. Other long-term costs will include software monitoring to deal with patches, upgrades, and updates; warranty and indemnity rights and obligations; confidentiality and intellectual property rights and obligations, and more. It will also be critical to investigate the option of insurance, both from a recall and cyberliability perspective. After all, suppliers and licensors will be at risk of being held responsible, even in the event of an accident or property damage claim.

Issues with hacking and data breach are only increasing and need to be addressed in your terms and conditions and supply agreements. Review your customer's requirements with an eye towards what potential liability you may have in the case of a data breach and cascade your risk to any vendors who may provide content, code or hardware that may assist in transmitting malicious programs. Of course, involve your counsel early and often in the negotiations and contract formation stages. An ounce of prevention is worth a pound of cure.

5. The abundance of collected data will lead to all kinds of increased risks

Not all hacks will be life-threatening attempts to take control of a vehicle. With a wealth of data available in the vehicle and through its content providers, it is possible that hackers will exploit connected vehicle systems. This content, including a driver's location data and preferences and other

data that serves to “improve the driver’s experience” is a treasure-trove to third parties that is often unprotected and an area where drivers cannot currently opt-out of collection. As seen in recent data breaches, these issues can be costly and detrimental to business operations. Implementing privacy and security by design and security can mitigate some of this risk.

Overall, companies in the connected technology sector are encouraged to consult with privacy, cybersecurity, regulatory and content management experts in order to take appropriate action on this growing threat.