Compliance & Ethics Professional®

June 2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Kristy Grant-Hart

Owner of Spark Compliance Consulting

Author of *How to Be a Wildly Effective Compliance Officer*

London, UK

See page 14

25
Put compliance chores on your To Do list
Les Abromovitz

29
Privacy in the European Union: A data safekeeping revolution
Daniel A. Cotter

33
The UK's new Modern Slavery Act and transparency in supply chains
Sarah Powell

37
Compliance officers share six strategies to boost compliance on a budget
Monica Modi Dalwadi

by Walter E. Johnson, CCEP-I, CHC, CHPC; Frank Ruelas; and Cindy Hart, LPN, CPA, CPC CHC

SPY Car Act: Navigating the automotive industry

» The Security and Privacy in Your Car Act was introduced in July 2015.

» Motor vehicles are vulnerable to security and privacy breaches.

» Automakers established a group to address security and privacy concerns.

» Autonomous vehicles are beyond the development of ethical decisions for driving scenarios.

» The Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers, Inc. have introduced the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services.

Decades ago, the automotive industry predicted that technological advances would transform how vehicles traveled. Evolving technologies are transforming dashboards into simulated cockpits, with long-term objectives of daily commutes occurring in the sky. In the meantime, the future is unfolding as drivers are soon to become passengers of autonomous vehicles. Automotive enthusiasts and collectors may experience legislation that prohibits traditional driving on roadways. On the other hand, those who are dependent on caregivers for travel will have more independence. Before engaging into the distant future, let's observe today's conditions.

Consumers have access to vehicles that have wireless Internet, remote start, navigation, voice recognition, self-parking mechanisms, night-vision cameras with head-up display, live roadside assistance, traction control, and an ongoing list of amenities. These amenities are driven by consumer demand to have their vehicles conveniently adapt to driving requirements. Also, it is how automakers maintain consumer demand for products in the maturity stage of the product life cycle. As technology makes it more convenient to remain connected and conduct business from virtually anywhere, risks are increasing as cyberattacks are increasing internationally. On average, organizations can expect to have hundreds of cyberattacks per day.

In July 2015, Senator Ed Markey (Dem-MA) introduced the Security and Privacy in Your Car Act, which is being referred to as the SPY Car Act.[1] The purpose of this Act is to protect consumers and passengers from potential harm as a result of cyberattacks to their vehicles. Markey is raising awareness to regulators, politicians, automakers, and consumers of the risks associated with data gathering and data transmissions performed

Johnson

Ruelas

Hart

by modern vehicles. The Act includes recommendations that require informing consumers of the potential for a vehicle's control systems, such as braking, steering, and acceleration being vulnerable through their connection to the vehicle's computer system.[2] Senator Markey recommends automakers design vehicles so that consumers are able to maintain control of the vehicle if it becomes a target of a cyberattack. The Act requires automakers to ensure that vehicle systems are not connected to major controls that may compromise the driver's ability to remain in control of the vehicle. Automakers are required to install a decal informing occupants that the vehicle is equipped with a cyber dashboard.

The introduction of the SPY Car Act is great timing. The past decade has been a rollercoaster ride for the automotive industry. It started with the government's bailout program. Since then, attention has shifted from preventing this domino effect to preventing other domino effects within the industry. Lately, there has been focus on quality and safety. High publicity associated with General Motors' faulty ignition switches, Toyota's faulty components causing unintentional acceleration, and Volkswagen's emissions scandal continues to unravel. These events require restoration of consumer confidence in the automotive industry. The Act gives automakers time to address risks before they evolve into compound issues.

The introduction of the SPY Car Act is great timing. The past decade has been a rollercoaster ride for the automotive industry. It started with the government's bailout program.

How widespread is the potential for vehicles to be hacked?

Prior to introducing the Act, Senator Markey sent letters to major automakers to discuss their actions to secure vehicles from hacking attacks and manage personal driving information. He received responses from 16 of 20 automakers.[3] The responses varied from brief overviews to detailed responses; the internal controls varied among automakers. This is not surprising, because cybersecurity remains underdeveloped. There is not a stand-alone regulation, but multiple sources are providing direction on cybersecurity.

Senator Markey summarized his findings and released the report, "*Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk.*" The report describes the current state of affairs; automakers have a long way to go to safeguard data and protect vehicles against cyberattacks. Notable highlights from the report include:

- Only two of the 16 automakers queried could describe any capabilities to detect to a real-time attack;
- Data collected on vehicles is not secured; and
- Individuals are often unaware of the data collection that is occurring.

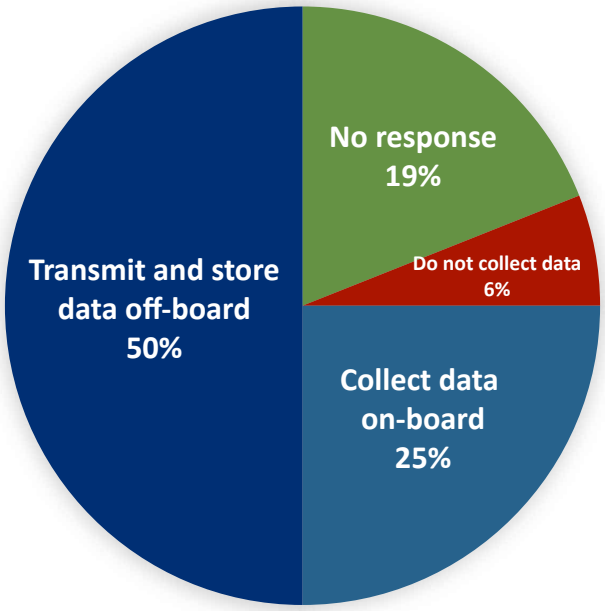
How widespread is the potential for vehicles to be hacked? The question is hard to answer definitively.

High-level points from the Act

Given the number of electronic control units that are vulnerable and how hacking may put the occupants of a vehicle at risk, it is no surprise that the SPY Car Act directs the Federal Trade Commission (FTC) and the National Highway Traffic Safety Administration (NHTSA) to enforce regulations to require automakers to protect their vehicles against cyberattacks. Senator Markey offers several recommendations to help minimize privacy and security threats to vehicle occupants:

- All entry points to electronic systems of motor vehicles manufactured for sale in the United States must be equipped with reasonable measures to protect against hacking attacks.
- Reasonable measures must incorporate isolation measures to separate critical software systems from non-critical software systems.
- Reasonable isolation measures must be evaluated for security vulnerabilities, following best security practices, including appropriate applications of techniques such as penetration testing.
- Any motor vehicle that presents an entry point must be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.
- All motor vehicles must display a "cyber dashboard" warning as a component of the label affixed to each motor vehicle.
- Manufacturers must inform consumers, through an easy to understand, standardized cyber dashboard graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements.

Figure 1 – Percentage of Automobile Manufacturers that Collect and Transmit Driving History Data



Privacy

Automakers are designing vehicles to collect information. The objective of data collection is to contribute to the process of improving the driver experience and vehicle performance. According to Senator Markey's research, 25% of the vehicles on the market collect data on-board, 50% transmit and store data off-board, 6% do not collect data, and 19% of the automakers surveyed did not respond to the questions.[4] (See Figure 1) The percentage of vehicles that can record driving history has either remained unchanged for some automakers or

increased for other automakers.[5] (See Figure 2).

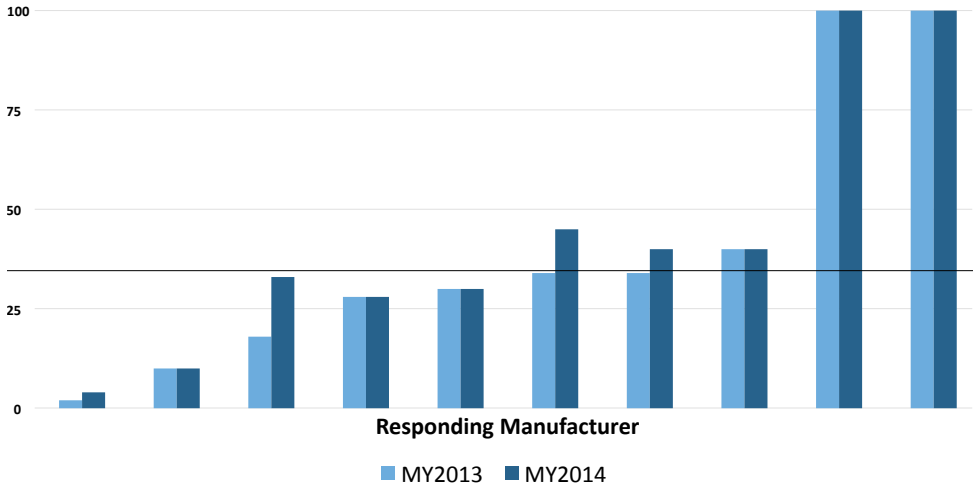
Driving data includes vehicle status, geographic location, and operational information. Examples of driving data include, but are not limited to, fuel level, battery health, tire pressure, error/fault codes, last location parked, vehicle's physical location, vehicle speed, and destinations entered into navigation system.[6]

Similar to mobile devices, consumers require education on location features. There are mobile device users who have fallen victim to unlawful acts, such as stalking, as result of their lack of understanding how to disable location features on their mobile device. Many mobile device providers offer user-friendly courses to educate their consumers.

Automotive consumers will require the same education. Understanding how to disable location services and erase personal data, such as destinations entered or driving patterns, is useful for safeguarding information. Senator Markey proposes that automakers design motor vehicles that allow occupants to disable location features without impacting navigation systems or other vehicle amenities.

Some automakers provide concierge services, such as dinner reservations, concert ticket purchases, and medical emergency calls. These services may require some exploration. For example, if a driver or passenger requires emergency services, they contact their concierge service provider and discuss their need for medical services. They are transferred to a 2-way call or 3-way call that includes an emergency medical provider. These calls will likely include protected health information (PHI). If PHI is collected onto a vehicle's computer system and later falls victim to a hacker, there may be potential breach considerations.

Figure 2 – Percentage of Vehicles that Can Record Driving History



This seems like déjà vu. Often, we hear advice suggesting observation of other industries that are managing the same issues to help your own industry. The automotive industry is in a prime position to consider lessons learned from healthcare compliance professionals. In fact, it appears that this may already be occurring. In particular, the health industry applies regulations to protect the privacy of health information.

The SPY Car Act will include requirements for automakers to install a cyber dashboard that provides the operator of the vehicle with information on those safeguards. Onboard safeguards are designed to protect access to information related to the operation of the vehicle. In addition, there will be an

"opt out" provision for owners or lessees of vehicles impacted by the SPY Car Act.[7] For those compliance professionals who work in healthcare, these two aspects sound interestingly similar to the Notice of Privacy Practices and the option for individuals to opt out of allowing their information to be posted in facility directories.

Security

Security breaches have consumers worried—they do not trust organizations with their information. Feeling helpless, consumers reluctantly provide the minimal information necessary to receive products and services. Consumer attention has focused on automakers' quality and safety, without major awareness of motor vehicle security breaches.

In Senator Markey's report, two studies are mentioned where researchers were able to control the motor vehicle's engine, brakes, steering, and other vehicle components by using a laptop to communicate with the computer electronic control units (ECUs) through the controller area network (CAN). In another test, researchers were able to increase acceleration, turn, disable brakes, activate the horn, control headlights, and modify the speedometer and gas gauge readings. Research included motor vehicles from 10 different automakers, and the security levels varied among automakers.[8]

Of Senator Markey's 16 respondents, only two automakers 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. Another finding is that the majority of automakers offer technologies that collect and wirelessly transmit driving history to data centers, including third-party data centers, and most do not describe effective means to secure the data.

The SPY Car Act will require automakers to reasonably secure all driving data collected by the electronic systems that are built into motor vehicles to prevent unauthorized access.

The SPY Car Act will require automakers to reasonably secure all driving data collected by the electronic systems that are built into motor vehicles to prevent unauthorized access. This applies to data stored on-board the motor vehicle, data in transit from the motor vehicle to another location, and any subsequent off-board storage or use. There are proposed penalties for violations.

Ethics

In several aspects, the introduction of the SPY Car Act reminds us of a challenge that not only exists in the Compliance arena, but one which significantly impacts the Ethics arena as well. This has to do with the ongoing development and application of technology as it outpaces the development of an ethical position on the use of this new technology. In addition, because an ethical framework or position has not been established, it is difficult to attempt to develop policies and procedures, which in turn support the compliance and ethics program of an organization. This is not a new predicament and is unlikely to vanish anytime soon, because it is well accepted that technology advances, particularly in the field of electronics, are not expected to slow down

anytime in the foreseeable future. In addition, the competitive nature of the automobile industry also serves as a motivating factor for manufacturers to design and implement new technologies in the design of their vehicles. This is not only for the purposes of making their vehicles operate more efficiently, but also to provide features that potential customers may find attractive as they consider which vehicle to purchase.

The ethics of hackers

The ethical dilemma of dealing with hackers is compounded by the unique attitudes and values that these individuals tend to share. For hackers, access to information that is supposedly protected and the consequences of accessing information are secondary to the reasons that hackers are a constant threat to those who try to protect information:

- Some hackers may be motivated by the opportunity of financial gain.
- Many hackers admit it is the thrill of being able to gain entry to information that is supposedly protected.

The ethical dilemma of dealing with hackers is compounded by the unique attitudes and values that these individuals tend to share.

Essentially, hackers and those who work to protect data against cyberattacks from hackers are in a constant battle where data security hangs in the balance. Sometimes hackers are successful in gaining access to data that has been secured, and sometimes they are not. We must realize that this ongoing back-and-forth between hackers and "anti-hackers" has moved into the realm of accessing automotive control systems, which can put occupants at risk. The anti-hacking community often recruits hackers to join the anti-hacking community. This is a result of continuous efforts by hackers to develop new ways to infiltrate systems, which is a valuable approach to develop methods to protect against hackers. In fact, this spawned a new occupation known as "ethical hackers." Ethical hackers work on behalf of companies by attempting to circumvent or bypass security measures. Ethical hackers help information technologists to close the gaps in security measures.

As this ongoing chess match between hackers and anti-hackers plays out, there seems to be little thought on the part of hackers on the implications or consequences of their actions with respect to the safety of those who may be occupants in vehicles that may be targeted by a cyberattack of the vehicle's control systems.

In a particular interview, a person (who was known to have developed techniques and technologies that allowed for the remote control of several of a vehicle's systems) made comments that indicated he did not perceive that taking control of a vehicle posed a particular risk to those who may be in the vehicle.[9] If this person's views are representative of the larger vehicle-control hacking community, it certainly seems that the ethical perspective of these individuals would not present much in the way of a deterrent or rational basis for them to consider that what they are doing is dangerous.

At the 2016 North American Auto Show in Detroit, John Krafcik, Chief Executive of Google's Self-Driving Car Project, shared how

self-driving cars are safer than other options and will drastically reduce vehicle deaths.[10] He adds, it can be incredibly dangerous when drivers resume control of the vehicle. Driverless vehicles may be safer as a result of technological advances that offer no distractions, better reflexes, and awareness (via networking) of other vehicles. At the moment, many automakers disagree with an autonomous approach, but support an incremental approach that includes options that allow the driver to resume control.

Collision-avoidance systems raise ethical concerns, also. There are complex scenarios that require human compassion, quick reflexes, and smart maneuvers. Here are a few scenarios worth consideration:

- Driver A's car is speeding along a bridge at 50 miles per hour when an errant school bus carrying 40 innocent children crosses its path. Should Driver A's car swerve, possible risking the life of Driver A, in order to save the children, or keep going, putting all 40 kids at risk?
- Driver A collides with Driver B. Driver A is slightly injured, but Driver B is moderately injured. Does Driver A's driverless vehicle remain stopped so that Driver A can check on the health status of Driver B and notify an emergency response team, or will the vehicle, if drivable, take Driver A to a medical facility while leaving Driver B?

Although speculative, these are scenarios that drivers may encounter during a daily commute.[11]

Collision-avoidance systems raise ethical concerns, also. There are complex scenarios that require human compassion, quick reflexes, and smart maneuvers.

As depicted on television, vehicle technology can be life-saving or life-threatening. In the television show, *Minority Report*, the police department was able to assume control of a vehicle from its reckless driver, suspend his license, and deem all of the owner's vehicles inoperable until suspension was lifted.[12] In *The Good Wife*, a law firm discovered a technical team seeking to prank a colleague had breached the driverless vehicle's systems. The prank was to include honking the horn and turning the windshield wipers on and off. This prank resulted in a rear-end collision that left another driver permanently paralyzed.[13]

Human ethics themselves are only a work in progress, and developing machines may require the coordinated efforts of philosophers, computer scientists, legislators, and lawyers.[14]

Navigating the way

During the development of this article, the SPY Car Act remained a bill. Despite its status, the Act is generating awareness. Activities that directly or indirectly support this bill are gaining momentum. For example, President Obama signed Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing. This encourages the voluntary formation of organizations engaged in sharing information related to cybersecurity risk and incidents to establish mechanisms to continually improve the capabilities and functions of organizations.[15] It requires organizations to conduct information

sharing in a manner that protects the privacy and civil liberties of individuals, preserves business confidentiality, safeguards information being shared, and allows organizations to share information.

An alliance of 12 automakers entitled, "Alliance of Automobile Manufacturers" (AAM) has committed to creating an information sharing and analysis center (ISAC). The center will let participating companies share cybersecurity data and keep each other aware of the latest hacking threats targeting vehicles. Additionally, there is a consensus among participants to limit the amount of data shared with technology companies. AAM anticipates automotive part suppliers, telecommunication providers, and technology companies to participate and contribute to this initiative. As a result of Senator Markey's research, AAM collaborated with the Association of Global Automakers, Inc. to develop the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services. Participating members agree to adhere to these principles as a commitment to deliver substantial benefits, enhance the driving experience, and retain consumer trust.[16]

California, Florida, Michigan, Nevada, North Dakota, Tennessee, and the District of Columbia have enacted legislature addressing driverless vehicles. In 2015, there were 15 states (including three carry-overs from 2014) that introduced legislation addressing driverless vehicles. Several states have multiple bills. Of a total of 22 bills, 12 failed, nine are pending, and one is substituted by another bill.[17] Preparations are underway and legislations vary by jurisdiction. Some states are developing legislation for street-testing, and others are developing legislation for the next phase.

Summary

The automotive industry is headed in a positive direction. These actions demonstrate their commitment in mitigating some of the known risks that cyberattacks present. Consequently, the automotive industry is investing resources, not only to develop vehicles that are safer from a structural standpoint, but also investing in ways to make their vehicles safer from cyberattacks.

It appears that the days of cyberattacks associated primarily with electronic data systems owned and operated by businesses within the financial, healthcare, and entertainment industries are numbered. Cyberattacks have taken on a new dimension—a dimension which now has entered the realm of the automotive industry, where it may have dire consequences with its potential for putting people in harm's way. ✳

1. Proposed House of Representatives Bill for the Security and Privacy in Your Car Act. Available at http://bit.ly/markey-senate
2. Senator Ed Markey: Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk. February 2015. Available at http://bit.ly/market-senate-2
3. Ibid, Ref #1
4. Ibid, Ref #2
5. Ibid, Ref #1
6. Ibid, Ref #2
7. Ibid, Ref #1
8. Ibid, Ref #2
9. Thomas Fox-Brewster: "SPY Car Act Hopes to Save American Cars From Digital Disaster" *Forbes*, July 21, 2015. Available at http://bit.ly/forbes-thomasbrewster
10. Mark Bergen: "In First Public Comments, Self-Driving Car CEO Urges Automakers to Buy into Google's Driverless Vision." *Recode*, January 12, 2016. Available at http://bit.ly/driverless-vision
11. Gary Marcus: "Moral Machines" *The New Yorker*, November 24, 2012. Available at http://bit.ly/moral-machines
12. *Minority Report*: episode, "The Machines Know All" aired October 5, 2015 on Fox Network Television.
13. *The Good Wife*: episode "Driven" aired November 15, 2015 on CBS Television.
14. Ibid, Ref #11
15. President of the United States. Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing. Federal Register. February 20, 2015. Available at http://bit.ly/cyber-info-sharing
16. Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc.: Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services. November 12, 2014. Available at http://bit.ly/alliance-of-auto
17. National Conference of State Legislators: Autonomous – Self-Driving Vehicles Legislation. October 7, 2015. Available at http://bit.ly/autonomous-2

Walter E. Johnson *(walter@wejohnson.org) is a compliance and ethics professional in North Potomac, MD.*

Frank Ruelas *(frank@hipaacollege.com) is Facility Compliance Professional at St. Joseph's Hospital and Medical Center/Dignity Health in Phoenix, AZ.*

Cindy Hart *(3cinful@gmail.com) is a compliance and ethics professional in Horsham, PA.*