BUSINESS LAW TODAY

Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?

Cheryl Dancey Balough, Richard C. Balough

About the Authors:

Cheryl Dancey Balough is the communications co-director of the American Bar Association's Cyberspace Law Committee and adjunct professor at Chicago-Kent College of Law. Richard C. Balough is the co-chair of the American Bar Association's Mobile Commerce Subcommittee of the Cyberspace Law Committee. Both are founding members of Balough Law Offices, LLC, a Chicago-based law firm that represents businesses in protecting and developing their intellectual property assets.

Today's cars are controlled by complex computer systems that include millions of lines of code connected by internal networks. Cars have become computers on wheels. The potential exists that a car's computers, like any computer system, can be hacked, leaving the car vulnerable to infection by malware. These vulnerabilities pose serious safety hazards should they be exploited nefariously. Legal implications of this technological vulnerability have yet to be adequately addressed.

Multiple Points of Entry into a Car's Computer Systems

Cars have dozens of electronic control units (ECUs) embedded in the body, doors, dash, roof, trunk, seats, wheels, navigation equipment, and entertainment centers. Common wired networks interconnect these ECUs, which also can connect to the Internet. This architecture provides almost unlimited gateways for external hacking and infection with malware. Some entry points to a car's ECUs require a direct, hard-wired connection, while others can be accessed wirelessly, including using Wi-Fi or RFID. Once entry is gained, a hacker can take over all of a car's computer-controlled systems.

In Austin, Texas, a disgruntled former employee of an auto dealer hacked into the dealer's computer system and remotely activated

the vehicle immobilization system, triggering the horn and disabling the ignition system in more than 100 vehicles. This anti-theft system had been installed by the dealer as a method of addressing non-payment by customers. While the anti-theft device was connected to the car's horn and ignition, the hacker did not take further control of the car.

Direct Entry via the OBD-II Port

All cars made after 1996 are required to have an Onboard Diagnostics connection (OBD-II) located within two feet of the steering wheel. All cars manufactured after 2008 must share the same OBD-II protocol. The OBD-II's initial function was to monitor mandated emissions equipment. Today, the port is used to monitor and control multiple functions. Service personnel plug equipment into the port for both diagnostics and ECU programming, typically via Windows-based computers, creating at least two paths for the introduction of malware.

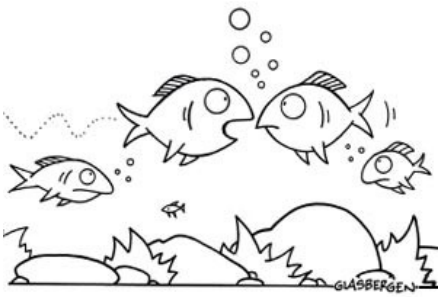
First, dealership computers typically connect to the Internet (and often are required by manufacturers to do so) for daily program updates. During that process, malware could be downloaded, infecting the computers. They in turn could spread the malware when connected to a car's OBD-II port. A second pathway is hacking into the dealership's internal wireless network. One university research team found that it was thereby possible to use the dealer's Wi-Fi to mount an attack.

More than dealers and mechanics use the OBD-II port. Parents can connect an app to the port to remotely monitor their children's driving, and fleet managers use apps to keep tabs on how their fleet vehicles are being driven. In addition to hackers intent on introducing malware, clever thieves can access the port to clone "smart keys" and simply drive away with a stolen car.

Remote Entry Points

The federal government also mandates that a car have an event data recorder (EDR), similar to an airplane's black box to record data about the status and operation of a car's systems. While historically EDR information was collected only via physical download, primarily to conduct a post-crash assessment, newer EDR systems permit data collection over remote wireless networks. The systems automatically transmit information to an emergency response center when an accident occurs. If the EDR can communicate via a wireless network to a data collection center, then malware similarly could be transmitted back to infect the EDR.

Entertainment systems, hands-free cellphone operations, and satellite radio also provide access points to introduce malware into a car's ECUs. For example, malware could be included in a



"Where is that retirement income stream I keep hearing about?"

SECTION NEWS

Earn Free Ethics CLE at In The Know - Cognitive Biases, Blind Spots, and Other Impairments of Ethical Vision: How Good Lawyers Can Go Astray
ABA Approves Section-Sponsored Resolution Opposing Burdensome New Tax Rules for Law Firms
Commercial Law Newsletter: Fall 2013 — Now Available
Spring Meeting Registration is Now Open
Business and Corporate Litigation Committee Newsletter: Fall 2013 — Now Available

All News

SECTION EVENTS

In The Know: Cognitive Biases, Blind Spots, and Other Impairments of Ethical Vision: How Good Lawyers Can Go Astray
December 17, 2013 at 1:00 p.m. Eastern
Webinar/Teleconference
Free for Section members, 1.5 ethics CLE credits requested

Cyberspace Law Institute & Winter Working Meeting
January 31 - February 1, 2014

CD inserted into the car's entertainment system. If an attacker can compromise a smartphone that uses a car's Bluetooth, the attacker can leverage the smartphone to compromise the car's telematics unit. Other paths to a car's ECUs can be accessed only at short range, such as remote keyless entry. Even tire pressure monitoring systems, which use wireless communication, are vulnerable and thus can open a pathway to the entire car's systems.

Car manufacturers are rushing to add new Wi-Fi functions as selling points. General Motors announced that for 2014 it will offer 4G LTE wireless, allowing passengers to access a Wi-Fi hot spot for use by multiple portable devices like phones and laptops. In the past two decades, car manufacturers have begun offering remote telematics systems on their vehicles, such as General Motors' OnStar, Toyota's SafetyConnect, and Ford's Sync. These systems use mobile phone voice and data communication, in conjunction with GPS technology, to give drivers hands-free remote access to emergency services, vehicle diagnostics, directions, and e-mail access. These services continue to evolve and now enable security measures such as remote ignition block and remote deceleration of a stolen vehicle. Computer scientists have demonstrated the ability to hack into such cellular-based telematics systems, transmit commands to vehicles, and surreptitiously listen to interior vehicle conversations.

Total Access All of the Car's Computer Systems

Because all of the car's ECUs are interconnected, once an entry point is found via any ECU, a hacker can access all car systems. While the Austin, Texas, incident demonstrates the vulnerability of a car's computer systems in a relatively benign way, not all hackers will be so restrained. Computer scientists at the University of California, San Diego, and the University of Washington conducted multiple experiments using various remote access modalities. For every vulnerability demonstrated, they could take complete control of a vehicle's systems – both while at rest and when traveling at high speeds. In addition, by hacking a car's computer, a thief could remotely unlock a car's doors, turn on its engine, arrive at the car's location, and drive off.

Even more menacing is automobile cyberterrorism, through which a terrorist could control cars via malware, using many of the same techniques for hacking into regular computers. This vulnerability could create mayhem on the roads if a hacker broke into a vehicle network and "ordered" car ignitions to turn off or brakes to engage or disengage. In 2010, the United States and Israel allegedly created the Stuxnet worm, which reportedly destroyed 1,000 centrifuges Iran used to enrich uranium by taking over the computerized systems operating the centrifuges.

Denver, CO
Four Seasons Hotel

Mergers and Acquisitions Committee Meeting
January 31 - February 1, 2014
Laguna Beach, CA
The Montage

Business Law Section Spring Meeting
April 10 - 12, 2013
Los Angeles, CA
JW Marriott Los Angeles at L.A. Live and the Ritz-Carlton Los Angeles

All Events

COMMITTEE NEWSLETTERS

Cyberspace Law
November 2013

Director and Officer Liability
November 2013

Business and Corporate Litigation
Fall 2013

Business Bankruptcy
October 2013

Legal Opinions
Fall 2013

All Newsletters

OTHER NEWSLETTERS

Miscellaneous IT Related Legal News (MIRLN) 13 October - 2 November 2013 (v16.15)

ABOUT BUSINESS LAW TODAY

BLT is a web-based publication drawing upon the best of the Section's resources, including featured

Stuxnet alerted critical infrastructure providers to the lack of protection from basic hacking. Automakers are no different than other infrastructure providers and are similarly vulnerable to cyberterrorism.

V2V and Self-Driving Cars

The potential vulnerability of cars to hacking will increase as vehicle-to-vehicle (V2V) and self-driving cars become available. V2V communication allows vehicles to send each other via Wi-Fi information such as location, speed, and direction of travel. Other data that may be exchanged include lateral acceleration, longitudinal acceleration, throttle position, brake status, steering angle, headline status, and the number of occupants in the vehicle.

Companies are gearing up for the V2V market. Google has been testing cars controlled solely by computers. Ford Motor Company expects to launch such cars by 2017. Two states, Nevada and California, have passed legislation allowing driverless cars on their roads. It is estimated that by 2040, self-driving cars could account for 75 percent of road traffic. At the 2013 Detroit Auto Show, Audi demonstrated a self-parking car, which one can retrieve from the garage via smartphone.

Industry and Government Addressing the Threat

One security expert estimates that the average auto maker is about 20 years behind software companies in understanding how to prevent cyberattacks. Like many computer systems, car computers previously were "air-gapped" from the Internet but are now connected via cell phones, Bluetooth, computerized diagnostic systems, and other exposed entry points. As long as the ECUs were not connected externally, the danger of introducing malware into a car was low and, as a result, the need to have sophisticated and updated security controls remained a low priority. Given today's connections, however, control systems must be designed to thwart cyberattacks.

This very real threat has prompted both the auto industry and the government to begin taking action. General Motors has a patent application pending for remote reprogramming of vehicle flash memory using digital satellite broadcast or other wireless transmission to the vehicle, thereby closing any "air-gap" between the car's ECUs and the Internet or any potential cyberattacker. SAE International, North America's largest automotive trade group, formed a special committee to draft new standards for security measures in automotive electronic systems. The U.S. Department of Transportation also is revising its testing procedures for automotive electronics.

Until industry-wide standards are adopted and implemented,

cars, their owners, and their passengers remain vulnerable, creating liability concerns for the automotive industry. If a malware attack were to occur, vehicle owners might be able to assert causes of action for defective design under state laws and for breach of implied warranty pursuant to the federal Magnuson-Moss Act. Most states have consumer protection laws targeted at unfair methods of competition and unfair or deceptive practices. These statutes might create a duty to disclose an objective, identifiable safety risk to consumers. California courts have found that defects in automobiles that could cause sudden or unexpected engine failure while driving pose such a risk. Evidence that a defect causes car engines to shut off unexpectedly or causes individuals to stop their cars under dangerous conditions also can trigger the duty to disclose.

In a class action involving plastic coolant tubes that cracked, leaked, or otherwise failed in a car, the plaintiffs alleged that the defendants knew, reasonably should have known, or were reckless in not knowing about the coolant tube defect but failed to disclose the defect to consumers. The court found the allegations were sufficient to sustain causes of action under many state consumer protection acts. The court also found that the Magnuson-Moss Act claims required that the warranties be determined by state law, and the court conducted a state-by-state analysis, finding the allegations sufficient in some states but deficient in others.

Similarly, if a court were to find that an auto maker knew or should have known about its cars' vulnerability to hacking and should have disclosed that vulnerability, then a consumer might have a cause of action under consumer protection laws. As for a breach of implied warranty claim, cars generally have warranties expressed in a number of years or miles. There is no specific "shrink wrap" type of agreement for the millions of lines of code in today's cars. If a court were to find an implied warranty that runs with a car's ECUs, then this cause of action might also exist for consumers if their cars are hacked into and controlled by malware.

Consumers whose car ECUs are compromised might alternatively sue auto makers under a defective design theory. Toyota owners took this approach after their vehicles suddenly accelerated. The court denied Toyota's motion to dismiss finding the complaint supported a design-defect claim given that the cars "do not meet consumer expectation because they suddenly and unexpectedly accelerate and cannot be stopped upon proper application of the brake pedal, [causing] crash and injuries." The court also denied Toyota's motion to dismiss a count for "warning defect theory," which allows for a cause of action even though a product is manufactured or designed flawlessly if the manufacturer later

learns there is a product defect.

While auto companies may argue that the threat of a third party inserting malware into a car and taking it over is beyond their control because it is external, similar arguments in the past have been rejected. Otherwise, courts have noted, all defective designs would be characterized as external even if they are predictable. Similarly, in the case of a malware invasion through inadequately protected points of entry to a car's systems, the threat is not just external, but predictable. By failing to protect the car's systems from malware, the predictable consequences are potentially disastrous and car companies might be liable for defective design of the computer systems without adequate protection in light of known cyber threats.

Protected Computer Under the CFAA?

Even with the efforts of multiple groups to thwart automobile cyberterrorism and other malicious attacks on car computer systems, the past couple of decades have taught us that hackers will always try to stay a step ahead. It is important to determine whether existing laws provide viable means to address hacking into automotive computer systems as a civil cause of action or criminal offense.

If a hacker or terrorist gains access to a car's ECUs and installs malware, that insertion would be without authorization under the Computer Fraud and Abuse Act (CFAA). The ECUs meet the CFAA's definition of a "computer," that is, the ECUs are high speed data processing devices performing logical, arithmetic, or storage functions. More problematic, however, is whether a car and its ECUs meet the definition of a CFAA "protected computer." In order to qualify, the car or ECU must be a computer "which is used in or affecting interstate or foreign commerce. . . ." Cars do travel in interstate commerce, but does the computer system affect interstate commerce as defined under the CFAA? At least one court found that in order to qualify as a protected computer, a computer must be used in interstate commerce. In other words, if the computing activity at issue takes place entirely within one state, the computers are not used in interstate commerce.

Even if a car itself is not a protected computer, the pathway to hacking a car's ECUs might involve a protected computer. If a person takes a car to a dealership for routine maintenance, a dealer's infected diagnostic computer could introduce malware into the car through its OBD-II port. Because the dealer's computer connects to the Internet, it is a protected computer under the CFAA. Similarly, a person may subscribe to an auto insurance company's program that monitors car usage to reduce premiums. The insurer tracks the car's usage in part by attaching a monitoring device to the OBD-II port. If the insurer's computers

are hacked to plant malware aimed at cars, this malware could be transferred in violation of the CFAA when the insurer's computer connects to the insured's car – a use in interstate commerce.

Whether or not the CFAA applies, car dealerships and insurance companies need to determine how they will address hacking. If a dealership or insurer discovers its computer system has been compromised to the point of infecting car ECUs, disclosure of the incident might not be mandated under state laws because the breach does not involve personal information. Given liability concerns, however, disclosing the security breach to car owners might be wise.

The DMCA and Protection

Assuming some software programs used to operate a car's systems are copyrighted and automakers have taken measures to prevent access, hacking into a car might violate the Digital Millennium Copyright Act (DMCA), which prohibits circumvention of technological measures to gain access to a copyrighted work. The DMCA's anti-circumvention provision creates a separate cause of action even when no copyright infringement exists. The Ninth Circuit found a violation of this provision in *MDY Industries, LLC v. Blizzard Entertainment Inc.*, 629 F.3d 928 (9th Cir. 2010). However, the appellate court declined to grant the plaintiff relief because the technology used to prevent access was not an effective access control measure. In reaching its decision, the appellate court cited a Sixth Circuit case, which found that to qualify under the DMCA, the technological measure must effectively prevent access. Therefore, a party seeking to use the DMCA to pursue the hacker of a car's ECUs would need to show that its car has technological measures that effectively control access.

Possible Violation of the Wiretap Act

Hacking into a car's ECUs might not by itself be a violation the Wiretap Act, but how a hacker inserts malware into a car's ECUs could violate the act. The Wiretap Act prohibits intentional interception of an "electronic communication," which it defines as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature *transmitted* in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). A hacker's interception of signals or data transmission between the ECUs *within* a car arguably would not affect interstate commerce. In addition, insertion of malware into a car's internal networks through its OBD-II port, a DVD, or a USB drive connected to a mechanic's diagnostic system without interception of data would not implicate the Wiretap Act because no interception occurs. However, if a hacker actually intercepts

an electronic transmission, e.g., a diagnostic system update from a manufacturer to its dealers transmitted via the Internet, in order to insert malware into the transmission, then the hacker arguably violates the Wiretap Act.

Intercepting transmissions from a vehicle also would violate the Wiretap Act. The act excepts from coverage certain types of electronic communications, including "an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." At least one court, however, has found that the ability for someone with specialized equipment to remotely capture data transmitted from a computer does not mean such data transmissions fall under the readily accessible exception of the act.

In an interesting twist, the Ninth Circuit found the operator of a vehicle monitoring system could not be ordered, pursuant to the Wiretap Act, to assist the Federal Bureau of Investigation (FBI) in monitoring conversations inside a car. *The Company v. U.S.*, 349 F.3d 1132 (9th Cir. 2003). One feature of the OnStar system allows the system's operator to open a cellular connection and listen to communications in the car. A purpose of this feature is to overhear thieves after a car is stolen to aid in the vehicle's recovery. Upon FBI's request, a district court issued several ex parte orders to allow eavesdropping under the Omnibus Crime Control and Safe Streets Act of 1968. The court found the monitoring service fell under the definition of the statute and required cooperation with law enforcement officials. However, when the OnStar listening feature was engaged, it disengaged other OnStar functions, including the button for automatic emergency response. On appeal, the Ninth Circuit found the lower court order invalid because it caused more than a "minimum of interference" with OnStar's services, so OnStar could not be ordered to comply with the FBI request.

How the Wiretap Act can assist law enforcement or civilians in addressing the vulnerability of a car's ECUs is not yet resolved.

Applicability of a Trespass to Chattel Tort Theory

A cause of action for trespass to chattel, governed by state law, might hold hackers liable for their activities. Generally, the tort requires intentionally dispossessing another of chattel, or using or intermeddling with chattel in the possession of another with resulting harm in the form of property damage or diminution of quality, condition, or value. An Illinois court found the plaintiff's allegation of trespass to chattel by defendant's installation of spyware on his personal computer was sufficient to withstand a motion to dismiss. *Sotelo v. DirectRevenue, LLC*, 384 F. Supp. 2d 1219 (N.D. Ill. 2005). Therefore, this tort might be a valid cause of action to employ in seeking damages from a hacker.

The PATRIOT Act

The PATRIOT Act and its extension modified numerous existing laws to protect against terrorism. However, the act does not address specifically cyberterrorism via cars. The act addresses terrorist attacks and other acts of violence against mass transportation systems, which are defined as passenger vessels, railroads, intercity bus transportation, school buses, and charter and sightseeing transportation, but it does not mention private passenger vehicles or trucks. The act also added to the punishment section of the CFAA offenses that are "a threat to public health or safety," but it did not otherwise amend the CFAA. As a result, the PATRIOT Act does not directly address car cyberterrorism.

Conclusion

Car makers are taking steps to reduce vulnerabilities to malware and cyberattacks that exist in their computers on wheels as they continue to roll out new products with even more technology. Legislatures and judges also will need to examine how today's laws apply to damage caused when hackers or terrorists exploit these vulnerabilities. These challenges will not disappear, but they might spawn a new industry: daily antivirus software updates for cars.