Planes, Trains, and Automobiles: a New Dimension in Cyber Conflict

Alessandro Guarino (StudioAG) and Emilio Iasiello (Looking Glass Cyber Solutions)

Abstract

Connected and Autonomous Vehicles (CAVs) are expected to garner an increasing share of the automobile market in the future and will combine with the introduction and diffusion of autonomous driving. What's more, vehicles will be integrated into Intelligent Transport Systems and Smart Cities. However, few studies have been conducted that take into holistic consideration cybersecurity, privacy and data protection; legal and regulatory implications; and the economics of this innovation. The present study explores how CAVs are powerful data generators and a fundamental element in the rapidly evolving Internet of Things. The paper builds on the definitions of "Connected Vehicle" and "Autonomy," moving from an overview of the IT technology on board modern cars, part of which is the basis for self-driving cars as well. It focuses on information security and cybersecurity, elements which until recently were not part of design requirements. The analysis also considers the huge economic ecosystem resulting from the opportunities to leverage the massive datasets generated. This ecosystem involves different actors with various interests and incentives, economic and otherwise, making for a very complex environment. The paper analyzes possible cyber economic warfare operations based on connected vehicles and will show how the privacy and data protection challenges stemming from CAVs interact with the security and economic aspects. The integration of individual vehicles into integrated systems brings into existence a novel dimension for cyberconflicts, supplying criminal organizations, terrorist groups, and state actors a host of potential targets, in addition to a remarkable source of extremely high-value data as well.

Introduction

Motivations and Scope

The expression "Internet of Things" (IoT) describes an environment where objects are connected to the global data exchange networks. Until recently, most Internet nodes were computers, servers, or smartphones. Today, however, objects of every kind produce and transmit data over the Internet, even if that is not their primary purpose. They run the gamut from Industrial

Control Systems (ICSs) to power distribution grids, to household appliances and toys. Persistent data exchange, most often bidirectional, between "smart" devices and remote servers not only opens huge opportunities but also presents challenges to information security, cybersecurity, privacy, and data protection. Perhaps the most relevant challenge of all is the potential to completely disarticulate traditional economic sectors and create completely new ones. Transportation systems, including connected and future autonomous vehicles, are a key element of this ecosystem, one of its focal points, and an extremely relevant part of developed economies.

The diffusion of Connected and Autonomous Vehicles (CAVs) overlaps with another important trend in the Information and Communications Technology field — the migration from "personal" computing towards remote and centralized services in the "cloud." This trend seems now irreversible, data protection and privacy concerns notwithstanding. It must be stressed that historically this is the negation of the "PC Revolution" that in the 1970s and 1980s put computing power in the hands of a huge number of individuals. Now the exact reverse is transpiring, where computing power is increasingly centralized in the hands of (a few) cloud operators. The convenience and marketing power of connected services trumps all other considerations. In light of this, we believe that, when it comes to vehicles, preliminary risk analysis should be more comprehensive than is currently the case.

A "connected vehicle" is any vehicle able to exchange data on the Internet (i.e., with Internet access, usually permanent). In most cases, this kind of vehicle also possesses built-in short-range wireless connections that can be used to connect with exterior devices and servers. Data exchange can happen with the manufacturer itself, with third-party cloud services, or with advanced Intelligent Transportation Systems (ITSs). Another useful classification for connected vehicles application is based on the number involved. Calendar alerts for users, maintenance alerts, and emergency localization systems are some typical "single-vehicle" applications. Examples of multi-vehicle applications include anti-collision and lane-change warning systems, car-sharing information systems, and city-level traffic optimization. Notably, connectivity can be retrofitted on existing vehicles as well (at least those manufactured since 1996, for cars) by installing simple devices able to access the on-board diagnostic (OBD) port, a widespread standard and one that is mandatory, at least in Europe.

Connected and Autonomous Vehicles: Definitions

Most technologies enabling connected vehicles are also leveraged by self-driving ones. In the latter's case, the software component is more complex and includes machine learning and artificial intelligence algorithms, among others. Theoretically, an autonomous vehicle (AV) should have no need to be permanently connected. However, command and control reasons and opportunities offered by the data exchange make it difficult to envision AVs as completely isolated.

The Society of Automotive Engineers (SAE) published a standard recognized as a reference to classify and study intelligent vehicles in which it defined “levels of autonomy”:

Level 0: No Automation. Full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems;

Level 1: Driver assistance. The driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task;

Level 2: Partial Automation. The driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving;

Level 3: Conditional Automation. The driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene;

Level 4: High Automation. The driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene;

Level 5: Full Automation. The full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.[1]

The Context

The CAV market is favorable, with some predictions estimating the number of IoT devices to reach 20.8 billion by 2020, according to the US research firm Gartner. The same organization estimated that approximately 250 million cars will be on the road by the year 2020. Over the past decade, the United States has seen an increase in the usage of AV technology in the automobile industry, on the back of research that has been developing for the past 45 years. This progress encompasses all aspects of computer technology, software engineering, and thought leadership on the part of such companies as Tesla, BMW, Ford, Audi, and even Google.

Advances in Artificial Intelligence (AI) have helped spur on CAV development. By its self-driving nature, a CAV must have the ability to operate independently, relying on surrounding environment situational awareness to navigate successfully. Sensors — 200 per car according to some estimates — provide the necessary understanding of the world around a CAV and a "brain" that processes collected data and selects a given course of action based on the processed information. Each CAV is outfitted with advanced tools to gather information, including long-range radar, laser illuminated detection and ranging (LIDAR), cameras, short/medium-range radar, and ultrasound.

The auto industry has been socializing CAVs to the broader market. Always on the forefront of innovation, the industry presents new automobile models to compete for market share. CAVs appear to be "the Next Big Thing" in automobile manufacturing (together with electric drive), presenting a variety of economic, environmental, and safety benefits for consumers. Moreover, CAV's technological makeup is an attractive selling point, demonstrating how the auto industry is keeping pace with the technological revolution and the interconnectivity that the Internet and computer technology affords. In an industry traditionally challenged to attract major

[1] SAE INTERNATIONAL Standard J3016.

software talent, automakers are hiring, opening or expanding existing Silicon Valley offices to attract and retain the software engineers they need to compete in the future.

Much expectation is placed on the CAV market, which is forecast to experience significant economic benefits. By 2035, more than 12 million fully AVs are expected to be sold per year globally. By 2035, 18 million partially AVs are expected to be sold per year globally. Moreover, the market for partially and fully AVs is expected to leap from about $42 billion in 2025 to nearly $77 billion in 2035, according to a 2017 study conducted by the global management Boston Consulting Group. The Brookings Institution supports these conclusions, believing that by 2040 AVs will comprise around 25 percent of the global market. IHS Automotive estimates that the US self-driving software and its corresponding updates will grow from $680 million in 2025 to $15.8 billion in 2040. The World Economic Forum estimates that CAVs will generate $67 billion in economic value and $3.1 trillion in societal benefits by 2021.

Moreover, there is significant value associated with the big data collected, produced, and processed by CAVs that can enable new business models. According to an IHS Automotive study, $14.5 billion of value from the Original Equipment Manufacturers connected car landscape is found in a connected car's big data assets — diagnostics, location, user experience (UX) /feature tracking, and adaptive driver assistance systems (ADAS)/autonomy. Considering that the Google self-driving car, for example, generates 1Gb of data per second, it puts into perspective the volume of data that can be produced, processed, synthesized, and integrated. A 2016 report by McKinsey & Co. estimated that the overall revenue pool from car data monetization at a global scale might range between USD 450 to 740 billion by 2030.

Nevertheless, challenges exist within the CAV universe, particularly with regards to standardization of how such vehicles are produced and the criteria to which they adhere. For example, many incorrectly assume that CAVs are all essentially the same, when there may be different technology and configurations at play. This raises the question of whether such technology should be shared and standardized to avoid the risk of society and/or policymakers not widely accepting CAVs on public roads.

Technological Context: The Internet of Things and Intelligent Transport Systems

Like many innovations born in the last decades, the IoT has roots in the military. The "Electronic Fence" was the brainchild of then-US Secretary of Defense Robert McNamara; its purpose was to block the flow of troops and supplies along the Ho Chi Minh Trail connecting North and South Vietnam. A classified DARPA project, the system would have consisted of a wide geographic network of sensors and actuators, all connected to a remote, centralized command and control center.[2] Though the goals are very different, this is exactly the idea behind the IoT. Ultimately, the "Electronic Fence" project never advanced even though the underlying ideas were not completely abandoned, evolving into what is now "network centric warfare." The maturation and commercialization of the Internet allowed the same idea to transition to the civilian world.

On modern vehicles, ICT are pervasive. No longer alone, Engine Control Units are now joined on the network by a host of other computers, morphing into the definition of "Electronic Control Units." Even the cheapest car is home to several, mostly interconnected, networks. The control area network (CAN) protocol is a specialized industrial protocol developed especially for the automotive industry. Widely used to connect critical elements of the on-board systems, starting with the engine and transmission, this bus-based network protocol used to be accessible only via the OBD port (this standardized access port is mandatory on all vehicles since the early 2000s). Linking this "core" network to other, less-critical systems seemed a natural evolution, but ultimately increased the attack surface from an information security perspective. Now there are several powerful processors connected in a complex local internetwork leveraging dated and insecure protocols and newer, standard protocols. Dozens of sensors produce hundreds of data types on all aspects of the vehicle; actuators operate everything from the steering wheel to the brakes, throttle, and gearbox. Sensors range from low-level parameter-reading (e.g. engine rpm, pedal, and other controls positions) to more complex inputs like video feeds, GPS receivers, or LIDAR used for AVs' navigation. All of this is accessible not only by connecting a physical device to a dedicated port but also through standard USB ports, and most importantly, via short-range Bluetooth/infrared from WiFi or high-bandwidth cell connectivity from everywhere. Physical access is not needed anymore.

[2] A. Jacobsen, *The Pentagon's Brain,* New York, Little, Brown & Co., 2015.

Currently, cars can be considered a true operating system, supporting the integration of the huge amount of data generated by its embedded sensors and complex application platforms. Examples of such platforms include General Motors' MyLink, Ford Sync, and Daimler-Benz's DriveStyle. The following is a useful classification of applications built on an enabling technological platform comprising sensors, actuators, and networks:

Service Packages: These packages complement or improve vehicle use, are sold by the manufactures, and follow the classic sale model of the "options" — a one-off payment. However, these packages will probably move to a fee-based model soon. Examples include anti-collision software and emergency assistance services.

Consumer Services: Most of these services are based on cloud connection. Examples include e-Commerce, multimedia streaming, social networks. These services will most probably still be supplied by the current suppliers or new-entrants, even if car manufacturers would be interested in including them in their bouquet. This category includes such applications as intelligent mobility systems, car-sharing providers, hotel, and restaurant recommendations.

Furthermore, connected vehicles will be an integral part of developing ITS and integrated into the wider concept of Smart Cities. ITS is the application of sensing, analysis, control, and communications technologies to ground transportation to improve safety, mobility, and efficiency. ITSs include a wide range of applications that process and share information to ease congestion, improve traffic management, minimize environmental impact, and increase the benefits of transportation to commercial users and the public in general. As defined by one company, ITS is composed of several components, including:

Vehicles: Motor vehicles, connected and autonomous, but also railway systems and other means of transportation;

Roadway Reporting: Data compiled from cameras and sensors and transmitted to control systems in order to make traffic movement more efficient;

Traffic Flow Controls: Monitors traffic and roadway conditions;

Payment Apps/Systems: Automatic payment to include tolls, kiosk payment machines, and e-tickets.

Management Apps/Systems: Controls all aspects of ITS from a centralized center.

Communication Apps/Systems: Facilitating the exchange of data. This is a fundamental aspect of ITS, because smart systems and smart cities need data to work. Security, privacy, and data protection of these massive datasets will be a key to their development.

Economic Context

1) The automotive industry

The industry is facing the saturation of most markets in developed countries. The rapid development of emergent markets, especially in Asia, is not enough to avoid a radical rethinking of the products and the sector itself. Growth slow-down, climate change, new regulations, and the need to move towards electric power have applied pressure to the producers and imposed huge investments. The industry consolidation process is still underway, as new entrants like Tesla are trying to leverage the technology shift. Opportunities stemming from the economic exploitation of big datasets generated by vehicles are too tempting not to be exploited by carmakers eager to bolster their profits.

2) Digital markets economics

According to a 2013 study by IHS Automotive, data exploitation will have generated $14.5 billion revenue by 2020. Big data offer a novel source of revenue for carmakers, but begs the question — who are the owners of the data? Ownership of car-related data is being debated between the various stakeholders, but chiefly between the car producers and digital companies. At the German manufactures' association VDA congress in 2014, then-CEO of Volkswagen Group Winterkorn said, "While [VW] will connect to Google systems, we want to be masters of [the data generated by] our cars." At the very same panel, Dieter Zetsche, CEO of Mercedes, stressed the high potential for conflicts around data sharing and use. Both digital operators and manufacturers are fighting over ownership and economic exploitation rights. A fundamental question on privacy and data protection remains unanswered in the European Union (EU), and the classification of some of the data as "personal data" is still an open problem.

Connected Vehicles as (Big) Data Generators

A Veritable Cornucopia

The variety of data that a CAV generates is astounding, generally falling into three main categories: raw data, derived data, and other information stemming from systems installed on the car or truck. Raw data are sensors' output before any elaboration (e.g., throttle and brake pedal positions, engine rpm, valve positions, etc.). These data are temporarily stored and not in an accessible way. Deducted information derives from an elaboration of raw data (e.g., fuel consumption per unit (km or mile), average speeds, etc.). Other information includes anything from base stations reached by the on-board SIM card to dash cams video feeds, GPS waypoints and itineraries, entertainment choices, and preferences.

Currently, the economic value of all these datasets is uncontested, and the various automotive ecosystem stakeholders — be they the new "digital" players or the established car makers — are keen to leverage them. While the danger for users' privacy is potentially significant, especially where personal data are not considered the individual's property, some attempts at self-regulation already exist. Worth mentioning are the "principles" developed by VDA in 2014 that try to reconcile business opportunities with applicable law and regulations. According to these principles, data "pertaining to the vehicle" are freely usable by the manufacturer, while other "user" data should remain under the control of the vehicle owner. Vehicle data comprise of raw and even derived data, which apparently are not considered "personal data." While a step in the right direction from the point of view of privacy protection, it is not enough, as privacy breaches could come about just by accessing raw data.

A 2015 experiment conducted by a research group from the University of Washington[3] highlights these risks. Researchers demonstrated how, using only raw data generated by regular on-board sensors from a stock 2009 sedan, it was feasible to identify the person driving the vehicle with a high level of accuracy. Data was recorded from 16 sensors producing 37 types of data and was structured into two different use cases: in the first scenario, the "subject drivers" made three laps around a closed lot, including parking and lane-changing maneuvers, and in the second, the

[3] M. Enev et al., "Automobile Driver Fingerprinting," in *Proceedings on Privacy Enhancing Technologies*, 2016 (1), pp. 34–51.

test consisted of a fifty-mile trip in normal traffic. Employing machine learning models to the datasets, it was possible to individuate the different driving styles with 100 percent accuracy. Obviously in this study the number of drivers was very small, but so was the size of the datasets, both in terms of number of sensors and of time. Nevertheless, the experiment showed that even with relatively small datasets it is possible to profile different drivers leveraging only raw technical data. Such an application could be considered a form of biometric identification.

The Data

CAVs must collect, process, and synthesize situational awareness data in real-time to be effective in navigating through complex environments more efficiently and safer than human drivers. As such, collected sensor CAV data are integral to the success of CAV implementation on a broader scale. Because the CAVs generate different categories of data, such information can not only be monetized but can also potentially yield significant profits in the future. According to the McKinsey & Co. study mentioned above, the market being created by access to massive amounts of car data is broadening the set of players in the car ecosystem, providing new sets of value creation models, and generating many (related) use-cases and monetization options.

Data generated by CAVs can be used in a variety of ways and are obtained via three primary methods: vehicle-to-vehicle; vehicle-to-infrastructure; and vehicle-to-sensor. These vectors facilitate the ability to collect and share information on roads, the surrounding environment, and other vehicles in transit via Dedicated Short-Range Communications. Based on the collection, processing, and synthesizing of these data elements, the CAV can navigate independently of a human driver.

Technology advancements have enabled CAV systems to integrate data to guide the operations of the automobiles. There are three main hardwares in the CAV model: sensors, processors, and actuators. Images and information gleaned from sensors travel through the processor, which effectively tells the car what to do via actuators — tools that allow a computer to control physical components like brakes, or steering wheels. Some of these technologies include:

Global Positioning System (GPS): GPS provides global location and time references of objects for accurate and constant position tracking;

Inertial Navigation System: This system monitors the positioning, direction, and speed of a vehicle with on-board motion and rotation sensors; and

Laser Illuminated Detection and Ranging (LIDAR): These sensors identify surrounding objects and/or environment with data for precision distance measuring.

The information collected and processed by these sensors is diverse and can include anything from planned routes, weather forecasts, fuel levels, and even information about the drivers' destinations. Additionally, CAVs can deliver notifications of traffic delays and provide alternate routes, as well as parking close by. The ability to tailor features to suit the driver's needs is one of the greatest strengths of CAVs. Micro-categories of CAV data include external and environmental conditions; the vehicle's technical status (e.g., oil temperature, airbag deployment); vehicle usage (e.g., speed, load weight, location); personal data and preferences (e.g., driver/passenger identity, use patterns of applications); and direct communications from the vehicle (e.g., calendar, phone, email).

Information Security and Data Protection

Cybersecurity of CAVs

The several gateways through which CAVs exchange information constitute their main weakness and multiply the exploitable attack surface. In traditional vehicles, physical access was necessary to interact with on-board networks and processors, whereas in CAVs remote access is possible. Moreover, the availability of wireless connections to the OBD port means retrofitting insecurity, thereby compounding the risk.

Software updating and patching is a critical area of concern. While CAVs share this with all IoT devices, the safety implications of a misconfigured or hijacked remote update raise the stakes. Typical owners are rarely up to the task of regularly updating their vehicle's software. The obvious alternative of automatic download and patching presents its own downsides (e.g., possible hijacking or impersonating safety considerations when the vehicle is in use), not to mention the problem of long-term support. On software updates, convenience typically trumps security. Vendors are aware of this preference but suffer from a low level of security awareness as well. This is due not only to lack of specific skills inside their organizations but also to powerful economic considerations. The need to bring to market new products quickly works against

incorporating security features. Therefore, it's unsurprising that there are vehicles with serious security defects like the connection between essential (e.g., engine and brakes) and non-essential (e.g., entertainment) networks. Lessons from automatic updates of smartphones could very well be applied to this context, since the level of security of those systems has reached at least an acceptable level.

A series of very public incidents over the past few years has affected the scenario as well. In 2015, researchers demonstrated how it was possible to remotely take control of a Jeep Cherokee SUV, causing it to veer off the road. As a result, FCA was forced to recall 1.4 million vehicles. Another victim was Mitsubishi's Outlander PHEV hybrid, in which the password for the onboard Wi-Fi network was the same for all cars and was printed on the user manual. Security researchers easily penetrated the system via Wi-Fi, reverse-engineered the internal communication protocol, and disabled the anti-theft system.[4] Finally, in the case of the Nissan Leaf, the car shipped with a useful remote-control app. However, the credential was the Vehicle Identification Number (and not editable), which is typically etched on the car's windows.

Despite the absence of any formalized binding regulations, there has been progress made developing a cybersecurity framework with regards to CAVs. At present, the Alliance of Automobile Manufacturers and the Association of Global Automakers have taken the lead in addressing data protection of CAVs, at least in the United States. The two organizations helped establish the Automotive Information Sharing and Analytic Center (AUTO-ISAC) to share information about vehicle-related cyber threats. While the organization does not have regulatory control over CAVs, it does provide a cybersecurity "best practices" document on its website that focuses on seven functions affecting vehicle cybersecurity.

The British Department for Transport also is aware of the risks and in 2017 released a set of key principles of vehicle cybersecurity for connected and automated vehicles:

Principle 1: Organizational security is owned, governed, and promoted at board level;

Principle 2: Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain;

[4] PenTestPartners Lab, "Mitsubishi Outlander Hack." Retrieved from https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/.

Principle 3: Organizations need product aftercare and incident response to ensure systems are secure over their lifetime;

Principle 4: All organizations, including sub-contractors, suppliers, and potential third parties, work together to enhance the security of the system;

Principle 5: Systems are designed using a defense-in-depth approach;

Principle 6: The security of all software is managed throughout its lifetime;

Principle 7: The storage and transmission of data is secure and can be controlled;

Principle 8: The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail.[5]

These high-level guidelines are very possibly well behind the curve in terms of what is possible in vehicle exploitation by hostile actors. A good example of this is "adversarial learning" attacks. AVs rely on machine learning, particularly so-called deep-learning algorithms, which can be tampered in many ways. For instance, the integrated vision component can be tampered with, impeding such functions as traffic sign recognition and classification. This can lead to the AV not respecting speed limits and, generally, behaving in dangerous and/or unpredictable ways.[6]

Cybersecurity of Intelligent Transport Systems

CAVs will be increasingly more integrated into the larger ITS and Smart Cities environments. As a critical infrastructure, ITS represent valuable targets for cyberattackers. As CAVs are a part of the larger IoT environment, they are equally susceptible to remote hacking, as well as physical operations, that seek to obtain gain unauthorized access. IoT devices have already been used to support some major cyberattacks as evidenced by the 2017 Reaper and the 2016 Mirai botnets. CAVs can be used in a similar manner. Cybercriminals have continually demonstrated ingenuity when designing and building their botnets, and while CAVs have not been abused in this

[5] United Kingdom Department for Transport. Retrieved from https://www.gov.uk/government/publications/principles-of-cybersecurity-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles.

[6] I. Evtimov et al., R*obust Physical-World Attacks on Deep Learning Models*, 2017. Retrieved from https://arxiv.org/pdf/1707.08945.pdf-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle cyber-security-for-connected-and-automated-vehicles.

manner, if security features remain weak, they may well be the next evolution in the construction of an IoT botnet. Ransomware, holding owners' hostage by locking them out of their cars, is just one way in which cybercriminals can profit from exploiting CAVs.

Given the fact that terrorists are using automobiles and trucks to conduct physical attacks, being able to control CAVs remotely provides these individuals with the benefit of not being physically present at the site of the attack. Furthermore, the exploitation of CAVs would allow terrorists to conduct several attacks at once and in different locations. The same can be done for railway systems, another favored target of terrorist attacks. Additionally, being able to control an individual's car may be a method by which terrorists seek to assassinate targets.

Moreover, the data produced by CAVs can be used to support intelligence collection. By compromising vehicles, outsiders may access important sensitive data such as GPS location, wireless communications, and, if other devices are connected to the automobile, data stored on handheld devices, laptops, or tablets. According to documents published by WikiLeaks, the US Central Intelligence Agency is alleged to have been seeking to be able to infect vehicle control systems used by modern cars and trucks.

Smart technology currently being deployed is not limited to cars or trucks. It's being leveraged in railway systems to better safeguard trains from collisions and improve transport efficiency. Many operations are now automated, and some are remotely controlled by computers. In 2016, a research group published its findings after a three-year study, which found many weaknesses that influence the signal and control systems of trains and the support systems for rail-related activities. The researchers found that while train systems are usually not connected to the Internet, security breaches of equipment and systems allow attackers to exploit these vulnerabilities and potentially carry out attacks on the railway system.

For example, European trains are controlled by the SIBAS system. Although generally deemed safe, a cybersecurity company has claimed that the WinAC RTX controller, one of the SIBAS components made by Siemens, is a security vulnerability. In the United Kingdom, the government published a Rail Cyber Security Guide in which it noted that the rail system was vulnerable to cyberattacks due to the transition to open-platform, standardized equipment built using commercial off-the-shelf components. This guide comes on the heels of four hacker attacks on the British rail network in 2015.

Privacy and Data Protection

1) The problem of data protection

CAV dataset exploitation is a potential threat to individual privacy, as evidenced in the 2015 incident above. Complicating matters is that discerning personal information from other kinds of data is now almost impossible given the availability of advanced machine learning models and algorithms. Data diffusion and information leaks compound this risk, as telemetry data can be combined with the personal data generated and stored on the car's communication and entertainment systems. Data localization bears noting as well, especially when vehicles travel across different jurisdictions, as privacy protection rules are not homogenous. Laws and regulations will have to develop and align with these new realities.

In general, users are not aware of the risks. In practice, notices of risk are not given to owners when they acquire a new vehicle, nor are they asked for their consent to allow their data to be collected. In terms of data retention policies, there is little consideration given to how information is disposed, deleted, or sanitized once a car is sold, a significant risk given the value that personal sensitive data has in the cybercriminal underground. Potential examples of privacy breaches include cases in which external subjects — legitimate or not — exploit vehicle data to learn information about the driver, the automobile, or both. Motivations are diverse, ranging from suspicious spouses, criminal information theft, blackmail, insurance investigation, or target surveillance and monitoring.

2) Europe and America

Jurisdictional fragmentation regarding privacy regulations is a source of friction in global markets and constitutes an added cost (and possibly an entry barrier) not only for the producers of connected vehicles but also for entities looking to leverage the data for their business. Adding to these challenges is the radical dichotomy between the EU and the United States, wherein privacy and data protection considerations are viewed differently. In Europe, data is the property of the individual and it can be processed only by consent. For profiling activities, special provisions are made in terms of consent and processing. The fragile "Privacy Shield" agreement now in force could very well face judgement from the European Court of Justice soon.

In contrast, in the United States, the commercialization of personal data is common practice. Still, while US legislation has not exactly made privacy a priority, several legislative

efforts have been made to address the challenge. Passed in 1994 and amended in 1999, the Driver's Privacy Protection Act first addressed the privacy of the driver, prohibiting the disclosure of personal information (defined in 18 U.S.C. § 2725) without the express consent of the person. However, with the volume of information being processed and transmitted with CAVs and CAV-related technology, the need for more robust regulation is required to bolster personal privacy. The current evolving regulatory framework for CAVs is being driven at the state level, defining rules that apply to the testing of CAVS on public roads. As of 2016, twenty US states introduced CAV-related legislation, with seven states enacting laws permitting testing on public roads. On a national level, there have been bills proposed that addressed data protection and CAVs. The two bills, both proposed in 2015 are:

> **The Security and Privacy in Your Car Act:** The bill directs the NHTSA and the Federal Trade Commission (FTC) to establish federal standards to secure cars and protect drivers' privacy. Under the SPY Car Act, the FTC would have to draft regulations to a.) require the notification of owners/lessees about the collection, transmission, retention, and use of driving date; b.) provide owners/lessees with an option to terminate such data collection and retention without losing navigation tools or other features; and c.) prohibit manufacturers from collecting information for advertising or marketing purposes without consent;
>
> **The Autonomous Vehicle Privacy Protection Act of 2015**: This bill is designed to protect consumer privacy during the development and use of CAV technologies by proposing the requirement of the Government Accountability Office to make publicly available a report that assesses the organizational readiness of the Department of Transportation (DoT) to address autonomous vehicle technology challenges, including consumer privacy protections.

At the federal level, the DoT has assumed a stewardship role for CAV development and deployment. In December 2016, the DoT proposed a rule mandating vehicle-to-vehicle communication on light vehicles, allowing cars to "talk" to each other to avoid crashes. It is hoped that the rule would advance the deployment of connected vehicle technologies throughout the US light vehicle fleet. On a separate but related track, the DoT's Federal Highway Administration

intended, as of this writing, to issue guidance for Vehicle-to-Infrastructure communications to facilitate communications between CAVs and infrastructure to improve travel and safety.

Finally, the National Highway Traffic Safety Administration (NHTSA) is responsible for developing and setting federal motor vehicle standards and regulations. In September 2017, the NHTSA published *A Vision for Safety 2.0,* updating previous NHTSA recommendations and promoting safety and mobility in AV deployment. The purpose of this Guidance is to help designers of automated driving systems (ADS) analyze, identify, and resolve safety considerations prior to deployment using their own, industry, and other best practices.

Conclusions

The automotive industry, so integral to modern economies, is undergoing a significant technical and economic paradigm shift. Convergence with the information economy is both a crisis and an opportunity for several interested stakeholders. Connected vehicles, integrated within ITS, will present a novel target for cyberattacks. ITS must be considered the quintessential public/private hybrid infrastructure, where all the questions on how to guarantee national security against hostile actors and how to protect citizens' civil liberties will come to a head. Currently neither the technical development of CAVS nor the regulatory efforts in this domain are sufficient to achieve those targets.

Security and data protection by design should both be implemented in the development of all components of smart transportation systems. Regulation efforts should be aimed towards both aspects of the problem and force the disparate actors (ranging from carmakers to municipalities) to implement them. At the moment, efforts are sparse and non-coordinated among different countries, limit themselves to cybersecurity only, or are too high-level and general. That is not enough, since the string of vehicle-based terrorist attacks in Europe and America in the last few years has patently showed the potential for hostile actions.