Connected Cars and Automated Driving: Privacy Challenges on Wheels

By: Peter J. Pizzi

Peter J. Pizzi is a business litigator with over 30 years of experience in commercial litigation, class action defense, internal investigations, internet and IP litigation, and labor and employment law. A founding member of Walsh Pizzi O'Reilly Falanga LLP, Mr. Pizzi has handled matters on behalf of corporate clients in a broad array of industries, including pharmaceuticals, insurance and financial services, advertising, social media, cosmetics, chemicals, industrial equipment, food service and others.

MUCH has been written in the technology press regarding issues of privacy, the connected car, and the promise of automated driving and other innovative mobility solutions. "Connected cars," which are on the road today in one form or another, merge the driver's digital world and means of transport. Automated driving, with the promise of true autonomous, self-driving vehicles, holds the potential in the near future to revolutionize the way people and goods move around. These developments, which challenge traditional ideas of tort and product liability and the insurance coverage that should apply, also loom as the cyber-criminal's new frontier and pose privacy challenges.

Why should any of these developments concern privacy? After all, device manufacturers equip today's smartphones with built-in geo-locating capabilities that enable numerous applications to track the user's every move, producing a rich stream of data which implicates the user's innermost thoughts. Apps added or activated by the smartphone owner enable the platform – either Google or Apple for most devices – to identify the movement of individual stocks in the owner's portfolio after the market closes each day or to inquire, "Are you at Le Pain Quotidien on 58th Street?" as lunch

is being served. Other apps collect the user's heart rate, level of stress, steps taken each day, and a myriad of other data. A connected car may get the user to a shopping mall, but smartphones know what individual stores a patron visits inside the mall, the aisles in the store that are browsed, and the articles of clothing considered for purchase, so that tailored ads, discounts, or coupons may dispatched the user's way. [1] How, then, could autonomous vehicles connected to networks and data centers via the cloud pose privacy challenges that haven't yet been addressed, if not resolved, in the operation of smartphones?

This article explores the subject of privacy, connected cars, and automated driving. Additionally, this article will introduce the reader to current approaches to privacy advanced by constituencies having a stake in the continued advancement of connected vehicles and automated driving.[2]

I. Defining Terms

Car connectivity generally comprises the sets of functions and capabilities that digitally and wirelessly link automobiles to drivers, services, and other automobiles. [3] Thus, a "connected car" generally refers to a vehicle equipped with technologies and services that transmit and receive data via wireless internet. The concept of a connected car is related to concepts of automated driving, which includes efforts to create autonomous driving and other innovative mobility solutions.

SAE International, the society of automotive engineers, anticipates connectivity and automated driving emerging and being deployed along a continuum of functionality. SAE therefore has developed a scale to describe that continuum, with the fifth level representing a completely autonomous vehicle. In late 2016, the National Highway Traffic Safety Administration ("NHTSA") adopted the SAE definition, which NHTSA then presented as follows:

---

[1] *See generally* David Brancaccio and Paulina Velasco, *How some retailers are tracking you as you walk down their aisles*, MARKETPLACE January 31, 2017, http://www.marketplace.org/2017/01/31/business/stores-are-tracking-you-and-consequences-arent-all-good.

[2] The author thanks Alma Murray, CIPP/US, Senior Counsel, Privacy, Hyundai Motor America, Timothy H. Goodman, Esq., Squire Patton Boggs (US) LLP, and Kurt B. Gerstner, Lee International IP & Law Group, for their invaluable suggestions in the preparation of this article.

[3] McKinsey & Company, *Connected Car, Automotive Value Chain Unbound*, September 2014 ("McKinsey"), at 1.2, available at http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/connected-car-automotive-value-chain-unbound.

There are multiple definitions for various levels of automation and for some time there has been need for standardization to aid clarity and consistency. Therefore, this Policy adopts the [SAE] definitions for levels of automation. The SAE definitions divide vehicles into levels based on "who does what, when." Generally:

- At SAE Level 0, the human driver does everything;
- At SAE Level 1, an automated system on the vehicle can sometimes assist the human driver to conduct some parts of the driving task;
- At SAE Level 2, an automated system on the vehicle can actually conduct some parts of the driving task, while the human continues to monitor the driving environment and performs the rest of the driving task;
- At SAE Level 3, an automated system can both actually conduct some parts of the driving task and monitor the driving environment in some instances, but the human driver must be ready to take back control when the automated system requests;
- At SAE Level 4, an automated system can conduct the driving task and monitor the driving environment, and the human need not take back control, but the automated system can operate only in certain environments and under certain conditions; and
- At SAE Level 5, the automated system can perform all driving tasks, under all conditions that a human driver could perform them.[4]

Many vehicles on the road today contain SAE Level 1 and Level 2 capabilities. Senator Markey's report titled "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk" and the recent National Auto Dealers

[4] At 8-9, available at https://one.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf.

Association and Future of Privacy Form's guide titled, "Personal Data in Your Car," [5] both conclude that vehicles on the road today have aspects of connectedness that place them well along the SAE continuum. For example, cars at the present time have on-board diagnostic information, apps (e.g., Apple CarPlay, Android Auto), location information available through navigation systems, and telematics services such as OnStar. With the SAE definitions in mind, an analysis of the impact of motor vehicle connectedness on the privacy of owners and occupants may be undertaken.

II. The Promise of Autonomous Vehicles

Vehicle connectivity and automated driving promise significant benefits as technology advances along the SAE continuum from today's Internet and app-equipped vehicles to SAE Level 5 autonomous vehicles.

NHTSA estimates that 35,092 Americans lost their lives in traffic accidents in 2015. The trend is not positive. It is getting worse. NHTSA also estimates that 27,875 Americans died in accidents in just the first nine months of 2016 alone. Globally, the World Health Organization estimates that 1.2 million lives are lost in crashes every year. These are numbers that could be reduced significantly with fully self-driving cars, especially since NHTSA estimates that 94% of crashes in the United States are attributed to human factors. [6] Consider the impact of autonomous vehicles on the blind, the elderly, the disabled, or those living with other conditions that make driving impossible. Infrastructure spending also could be diminished by connected vehicles, which make more efficient use of existing highways through closer operating distance between vehicles, improved ride-sharing, and other benefits.[7]

While there are some differences in the precise timeline, at present industry and technology leaders generally expect SAE Level 5 vehicles to arrive by 2025. [8] There

[5] Future of Privacy Forum, *Personal Data in Your Car*, available at https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf.

[6] Testimony of Dr. Chris Urmson, Director, SelfDriving Cars, Google [x] Before the Senate Committee on Commerce, Science and Technology Hearing: "Hands Off: The Future of SelfDriving Cars," March 15, 2016 https://www.gpo.gov/fdsys/pkg/CHRG-114shrg22428/html/CHRG-114shrg22428.htm.

[7] *Id.*

[8] *Global Automotive Industry Expects Self-Driving Cars on Sale by 2025, Says just Auto.com Survey,* DIGITAL JOURNAL quoting

are numerous competing platforms engaged in a pitched battle to commercialize self-navigation technology. In Singapore, a self-driving taxi service launched in August 2016.[9] The competition among Alphabet's Waymo, Uber, Tesla, and other firms is frenzied and has been widely covered in the business and mainstream media.[10] For example, in February 2017, Waymo sued Uber for theft of automated vehicle technology, and in March moved for a preliminary injunction against Uber and a former employee working for that company.[11] Waymo's motion papers described what is at stake in exciting terms: "Self-driving technology will revolutionize the way people and goods move around, generating untold revenues for those companies that successfully master it early."[12]

III. Consumers Today Are Concerned About Connectedness

Leaving the future for a moment, there is no doubt that today, consumers demand greater levels of connection between their automotive and digital lives, while at the same time appearing anxious about that very prospect. In 2014, McKinsey surveyed consumers about connected cars, finding that 37% were "highly concerned" about the digital safety and data privacy issues of connected cars such that they would consider not using a connected car because of those concerns.[13] The survey results appear to reflect consumers' instinctive recognition that if cars are connected in order to operate, literally everything that takes place with or in a vehicle will be captured electronically. In the case of fully self-driving vehicles, the data stream from the connected car will be constant in order for the vehicle to operate. But even today, the connectedness of new vehicles is considerable. Technologies that allow for safer, more convenient and entertaining vehicles amass vast databases of information about drivers, offering the potential to monetize that data by generating saleable insights. These insights can be used not only to improve vehicle systems and features, but also, if permitted, to track and profile customers for

---

just-auto.com, http://www.digitaljournal.com/pr/1975125.

[9] *See* https://futurism.com/the-worlds-first-autonomous-taxis-just-started-driving-in-singapore/.

[10] Alistair Barr, *Google's Self-Driving Car Project Is Losing Out to Rivals*, BLOOMBERG, September 12, 2016, https://www.bloomberg.com/news/articles/2016-09-12/google-car-project-loses-leaders-and-advantage-as-rivals-gain.

[11] *See* Complaint and other pleadings, Waymo LLC v. Uber Technologies, Inc., Civil Action No. 3:17-cv-00939 (February 23, 2017).

[12] *Id*. Waymo LLC Motion for a Preliminary Injunction, ECF No. 24 at 5 of 30.

[13] McKinsey, *supra* note 3, at 1.1.

targeted marketing and other purposes.

So, what are some scenarios in which connected cars implicate personal privacy? Today, some late model cars have the capability of reading text messages. Cars reading email correspondence cannot be far behind. If the data is merely passively read by the vehicle, and not stored, the privacy intrusions are mitigated. If the vehicle stores the data for some period, the impact could be more serious. Consider the driver who receives a work message while driving to the local Starbucks. Upon arrival, she orders a latte from the app on her phone. Her work-related communications and credit card information instantly enter and exit the car's computer. Depending upon the technology employed, ownership rights to that data, and its protection, as it passes through or is stored in the vehicle, implicate issues of personal privacy, corporate proprietary information, and data security.[14]

Other observers have conjured more prosaic, but equally important scenarios. A car company tracks a driver regularly visiting a cancer clinic.[15] The fact of those repeated trips could be of interest to various constituencies (e.g., a prospective or incumbent health insurer), but the data may be completely misleading, as perhaps the driver is a consultant working on a technology project for the medical provider. Who gets access to such records? Is such information subject to subpoena? The same driver has chosen to purchase new insurance for his vehicle and to allow the insurer to monitor his driving habits. If he decides to change motor vehicle insurers to obtain a better rate, can the new insurer gain access to his prior driving history as a condition of insuring him?

With each degree of connectivity, cars will become highly efficient data harvesting machines and a major element of the evolving Internet of Things. Each of these scenarios implicates a variety of legal regimes, ranging from expectations of privacy emanating from common law, HIPAA, the protection of trade secrets under state and federal law, state insurance laws, and numerous other regulations.

IV. What Law Applies?

Unlike in Canada or in European Union countries, the United States has no overarching law that covers all aspects of personal privacy. No single federal law or regulation governs the handling and securing of all types of sensitive personal

[14] KPMG, *Your Connected Car is Talking: Who is Listening?*, December 2016 ("KPMG"), available at https://home.kpmg.com/uk/en/home/insights/2016/12/your-connected-car-is-talking-whos-listening.html.

[15] *See id.*

information. Rather, on the federal level, U.S. privacy law has evolved in a sectoral approach, covering consumer credit, financial services, health care, government, securities, and Internet sectors. An example of this sectoral approach is the HIPAA Privacy Rule[16]adopted pursuant to The Health Insurance Portability and Accountability Act of 1996[17] to cover "protected health information." Financial privacy is regulated by The Gramm-Leach-Bliley Act[18] ("GLB"), which requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. [19] In the Internet sector, the Children's Online Privacy Protection Act ("COPPA") governs online marketing aimed at children.[20]

In the absence of a comprehensive federal statute governing personal privacy, forty-seven states stepped into the void, each with its own breach notification laws, [21] requiring organizations that suffer a data breach potentially to comply with conflicting and duplicative notification laws of dozens if not all forty-seven states. "Hodge-podge," "patchwork", and "mess" are terms that come to mind when considering the current state of affairs in regard to data privacy and breach notifications.

Federal regulatory enactments specific to personal privacy in the automotive realm include the Driver's Privacy Protection Act of 1994, which is not to be confused with the Driver Privacy Act of 2015. The former regulates the disclosure of personal information contained in the records of state motor vehicle departments, prohibiting such disclosure unless for a purpose permitted by an exception listed in one of 14 statutory subsections. The latter covers ownership of data recorded by monitoring devices, such as a vehicle's event data recorder ("EDR"), providing that ownership of that data vests in the owner of the vehicle or the lessor of the car, in the case of a rented vehicle.

Privacy in regard to connected vehicles appears ill-suited to state-by-state regulation, given that motor vehicles are by definition mobile, and manufacturers cannot be expected to design different

[16] 45 CFR Part 160 and Subparts A and E of Part 164.

[17] 104 P.L. 191, 110 Stat. 1936, enacted August 21, 1996.

[18] 106 P.L. 102.

[19] For a further explanation of the sectoral approach to personal privacy in the United States, *see* Congressional Research Service, *Data Security Breach Notification Laws* April 10, 2012, available at https://fas.org/sgp/crs/misc/R42475.pdf ("CRS").

[20] 15 U.S.C. §§ 6501–6506 .

[21] *See* Congressional Research Service, *supra n*ote 19 (surveying the forty-seven state enactments).

vehicles for different states. At the present time, an overarching federal privacy regime covering connected vehicles has not emerged, while the technologies are still in development.

V. SCOTUS on Vehicular Privacy

Consideration of how courts will deal with the phenomenon of connected, digitally monitored cars, generally begins with a discussion of the "reasonable expectation of privacy," which is the traditional standard used to resolve issues of personal privacy since the era of the Warren Court. The 1967 United States Supreme Court decision, *Katz v. United States*,[22] is credited with having originated the concept of reasonable expectations of privacy. In *Katz*, conversations recorded by police listening from outside a public phone booth were excluded from evidence, with the Court holding that the public location of the defendant did not vitiate his expectations of privacy because the Fourth Amendment "protects people, not places."[23]

Later decisions answered in the affirmative whether a "reasonable expectation of privacy" applies to individuals operating motor vehicles on public thoroughfares. In *Delaware v. Prouse*, the Supreme Court observed: "An individual operating or traveling in an automobile does not lose all reasonable expectation of privacy simply because the automobile and its use are subject to government regulation. … [P]eople are not shorn of all Fourth Amendment protection when they step from their homes onto the public sidewalks. Nor are they shorn of those interests when they step from the sidewalks into their automobiles."

In *U.S. v. Jones*,[24] the Court affirmed the suppression of evidence obtained by police through the placement of a GPS tracking device on the suspect's car. Though nine justices joined in the result, the reasoning was fractured. Five justices led by Justice Scalia relied upon a trespass-to-property rationale for the holding rather than the *Katz* expectation of privacy approach; the balance of the justices applied the *Katz* "reasonable expectation" analysis. Thus, the opinion may reflect a weakening in the adherence to *Katz* and its progeny. Post *Jones*, *U.S. v. Katzin*[25] represents the first relevant appeals court ruling to address the topic. The Third Circuit held that a warrant was indeed required to deploy GPS tracking devices and, further, that none of the narrow exceptions to the Fourth Amendment's warrant

[22] 389 U.S. 374 (1967).
[23] *See* Dorothy J. Glancy, *Symposium Article: Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1217 (2012).
[24] 565 U.S. 400 (2012).
[25] 732 F.3d 187 (3rd Cir. 2013).

requirement (e.g. exigent circumstances, the "automobile exception") was applicable.

Despite the fractured rationale on display in *Jones*, cases like *Katzin* have led one academic commentator to opine that courts are expanding rather than contracting Fourth Amendment protection for people in vehicles on public roadways and to forecast that recognition of reasonable expectations of privacy related to persons in vehicles on public roadways may well be unquestioned.[26]

VI. The Regulatory Perspective

Although the industry would prefer self-regulation (i.e., the Consumer Privacy Protection Principles discussed below), some form of federal pre-emption will be necessary in order to avoid the patchwork of laws that emerged in regard to breach notification. In the prior administration, regulators focused considerable attention on vehicle privacy issues. In September 2016, the U.S. Department of Transportation issued its Federal Automated Vehicles Policy,[27] which used the Federal Trade Commission's ("FTC") Fair Information Privacy Principles ("FIPP") as its guidepost. Such principles rely upon concepts of notice to the consumer, choice exercised by the consumer, access to data by the consumer, and cybersecurity protection of such data.[28] As part of the December 2016 NHTSA V2V (Vehicle to Vehicle) Notice of Proposed Rulemaking, NHTSA provided a Privacy Impact Assessment[29] which shows NHTSA's recognition of the privacy issues associated with V2V technologies and the tension between the benefits of new technology and personal privacy.

Further, any disconnect between manufacturer privacy policy representations and a firm's actual practices may draw the attention of the FTC, which has undertaken numerous court and administrative actions aimed at enforcing privacy commitments on the part of organizations. In so doing, the FTC has relied upon statutes such as the

[26] Glancy, *supra* note 23, at 1218-1219.

[27] The Federal Automated Vehicle Policy is available at https://www.transportation.gov/AV.

[28] The Fair Information Privacy Principles are available at https://web.archive.org/web/20100309105100/http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Notice/Awareness.

[29] *See* https://www.transportation.gov/individuals/privacy/vehicle-vehicle-v2vnprm-%E2%80%93-december-20-2016.

Fair Credit Reporting Act, COPPA, GLB, and other regimes, or upon the broad authority conferred by § 5 of the Federal Trade Commission Act,[30] which proscribes "unfair" and "deceptive" acts or practices affecting commerce. Such authority was recently given an expansive reading in the FTC's action against Wyndham Worldwide Corp. for its failure to implement reasonable data protection practices.[31]

VII. The Industry Response

In November 2014, participating members of the Alliance of Automobile Manufacturers and the Association of Global Automakers, a group of nineteen automobile manufacturers, published a set of Consumer Privacy Protection Principles, subtitled "Privacy Principles for Vehicle Technologies and Services." The Principles "apply to the collection, use, and sharing of Covered Information in association with Vehicle Technologies and Services available on cars and light trucks sold or leased to individual consumers for personal use in the United States." As might be expected, covered information means data "linked or reasonably linkable to i) the vehicle from which the information was retrieved, ii) the Owner of that vehicle, or iii) the Registered User."

The Principles obligate manufacturers to disclose to consumers the types of data collected and how that data is to be used or shared. Disclosure will be made in owner's manuals, on displays inside vehicles or on internet-based registration portals managed by the companies. Consumers will be able to review the policies before buying a car. The Principles cover the range of data that may be collected, including geolocation information, driver biometric data and driving behavior. To use any personal information for marketing purposes, car companies agree to first obtain permission from customers. Thus, before suggesting a restaurant along the route which the driver has entered in the vehicle, the driver would have to have given consent to receive such prompts. Automakers also commit to refrain from, for example, sharing driver behavior data with insurance companies without that customer's consent. The last commitment serves as some comfort to those with a heavy foot on the accelerator.

While the Principles provide a step toward the goal of having user privacy "baked-in" to connected vehicles, the document has received some criticism. In early 2015, the British Columbia Freedom of Information and Privacy Association published a 123-page document titled "The Connected Car: Who is in the Driver's Seat?" That document

[30] 15 U.S.C. § 45(a).

[31] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2016).

measured the automaker's privacy pledge together with privacy policies of individual automakers available online, against the dictates of Canadian data protection strictures.[32] Following that exercise, the BC group concluded: "The privacy pledge issued by a large group of major automakers in November 2014 is promising but falls far short of Canadian legal standards. In particular, it does not meet Canadian legal standards with respect to openness, accountability, individual access, consent, or limiting collection, retention, use and disclosure of personal data. Nor, in our view, does it meet the requirement for purposes to be limited to those that a reasonable person would consider appropriate in the circumstances."

In February 2017, the Future of Privacy Forum and the National Automobile Dealers Association released a consumer guide entitled, "Personal Data in Your Car" to inform consumers about the type of data collected by vehicles. Global Automakers and the Auto Alliance supported the publication. Press reception has been favorable.[33]

Manufacturers of connected cars are finding issues of choice challenging. For example, some privacy advocates urge that notice should be provided physically in the vehicle through interior displays as opposed to in the owner's manual or other methods. Providing a sequence of notices must be balanced against the NHTSA Distracted Driver Guidelines, [34] which call upon manufacturers to prevent utilization of certain secondary, non-driving devices which are believed by the agency to interfere inherently with a driver's ability to safely control the vehicle. A stream of notices, moreover, may have adverse consequences for the user experience. Displays for each potential occupant of a vehicle may

[32] As noted, the United States has no nationwide data protection regime similar to the Canadian or European models. Even so, such comprehensive privacy laws which are the norm outside the United States serve as a useful benchmark for the Principles.

[33] *See FPF, NADA release consumer privacy guide Biometric Update*, February 6, 2017, available at https://www.biometricupdate.com/201702/fpf-nada-release-consumer-privacy-guide *and* IAPP Daily Dashboard: *FPF, National Automobile Dealers Association announce car data Guidance*, available at https://iapp.org/news/a/fpf-national-automobile-dealers-association-announce-car-data-guidance/.

[34] National Highway Transportation Safety Administration, *Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices*, February 15, 2012, https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Distraction_NPFG-02162012.pdf.

also compromise the passenger compartment in unacceptable ways.

Car companies also are wrestling with how to provide notice to subsequent owners or purchasers of used connected vehicles. To achieve notice and consent, the manufacturer may have to track changes in ownership, which is not always possible for a distributor, even when this information is necessary for recall notices. NHTSA has challenged automakers to achieve greater accuracy in the delivery of recall notices, but changes of ownership remain difficult to track. The alternative appears to be in-vehicle display screen notices, which pose the challenges referenced above. Similar problems will be encountered in giving notice to drivers of connected rental cars.

A further privacy question involves ownership of the data stream itself. Is ownership vested in the vehicle manufacturer or the owner of the car? While the Driver Privacy Act provides that the data available in the EDR is the property of the owner or lessee of the car, such data may only be obtained by physical access to the car and represents only a snapshot in time (i.e. before airbag deployment). As such, EDR information pales in comparison to the other stream of information a connected, self-driving car can be expected to generate.

VIII. Securing That Data

In-depth consideration of the challenges of maintaining the security of connected car data is beyond the scope of this article. It must be recognized, however, that the flipside of connectedness is the challenge of securing the data – in other words, cybersecurity. As much as connected cars make sense to consumers who spend so much of their lives digitally connected, a hacked car[35] could prove a danger, potentially a weapon, and a means of destruction in the hands of highly sophisticated actors. Part of the process of building-in privacy protections involves ensuring the cybersecurity of connected vehicles. Fiat/Chrysler learned a costly lesson when it introduced a 2014 Jeep Cherokee with built-in Wi-Fi for passengers. In 2015, two ethical hackers hired by *Wired* magazine spent four months fashioning a "zero day"[36] attack against the vehicle. First, they infiltrated its cellular connectivity. Then they moved laterally to compromise the backbone of the car's electronics, called the controller area network bus (CANBus). Then they tapped the systems connected to the CANBus

[35] David Schneider, *Jeep Hacking 101,* IEEE SPECTRUM, August 6, 2015, available at http://spectrum.ieee.org/cars-that-think/transportation/systems/jeep-hacking-101.

[36] A zero-day attack is one that has never been seen before.

that control starting, stopping, accelerating, and steering, giving them complete control over the car while a *Wired* editor drove (or attempted to drive) the vehicle.[37] When the exploit was published, Fiat/Chrysler's stock price tumbled and it was hit with a class action.[38]

Dangers from the deployment of vehicles vulnerable to being hacked can hardly be understated. Connected vehicles will generate huge amounts of data, creating the potential for unwanted third-party access to that data, increasing the risk of a cyberthreat. A hack exposes personal data of a driver, such as location and potentially the identity of others in the car, enabling the perpetrator to know whose home may be unoccupied. Additionally, a hacked vehicle could have fatal consequences, not just for the driver and passengers inside the vehicle, but for anyone or anything physically surrounding the self-driving car.[39]

In October 2016, NHTSA published a paper entitled "Cybersecurity Best Practices for Modern Vehicles." The Best Practices document represents "non-binding guidance" offering "voluntary best practices" to improve motor vehicle cybersecurity. NHTSA calls for a "layered approach," adopting the National Institute of Standards and Technology ("NIST") Cybersecurity Framework[40] and its five principles: identify, protect, detect, respond and recover. NHTSA also calls for implementation of ISO 27000 series standards and like strictures, such as the Center for Internet Security's Critical Security Controls for Effective Cyber Defense. Although NHTSA concedes that these standards were developed to mitigate threats against networks and not necessarily automotive devices, it forecasts application of such protocols for use in the automotive industry. As with NHTSA's cyber-guidance for autonomous vehicles,[41] NHTSA also calls for information sharing among automobile manufacturers and the development of a process for vulnerability reporting.

---

[37] Schneider, *supra* note 35.

[38] https://www.bloomberg.com/news/articles/2015-08-04/hackers-force-car makers-to-boost-security-for-driverless-era. The class action was filed as Flynn v. FCA US LLC, Civil Action No. 3: 15-cv-00855-MJR-DGW, U.S.D.C., S.D.Ill. The case is still pending as of this writing.

[39] Chris Achatz, *Self-Driving Cars at a Glance,* (2015) http://www.bryancavedatamatters.com/self-driving-cars-at-a-glance/.

[40] Available at https://www.nist.gov/cyber framework.

[41] *See* https://www.huntonprivacyblog.com/2016/09/22/department-transportation-issues-cyber-guidance-autonomous-cars/.

IV. Conclusion

While it is difficult to find anyone happy with the patchwork that *is* the law of privacy in the United States, it appears premature to expect an overarching regulatory regime on the federal level to address privacy and data protection in the realm of connected cars. The industry is moving down the SEA continuum toward fully self-driving vehicles. But how the various 5th level self-driving modalities will look is conjecture at this juncture. Until we reach that point, courts will likely be called upon to address privacy concerns involving connected vehicles applying traditional privacy principles and existing regulatory structures.