McDermott Will & Emery

Special Report

A Short Primer on Autonomous and Connected Vehicle Regulation

McDermott Will & Emery

SPECIAL REPORT

For more information, please contact your regular McDermott lawyer, or:

Michael G. Morgan
+1 310 551 9366
mmorgan@mwe.com

Lynette R. Arce
+1 312 984 2759
larce@mwe.com

Amy C. Pimentel
+1 617 535 3948
apimentel@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com

Table of Contents

This article briefly introduces the emerging regulatory framework for autonomous and connected vehicles in the US and in certain key jurisdictions around the world, with particular emphasis on regulations pertaining to privacy and cybersecurity. Much of this framework consists of laws of general application that extend to autonomous and connected vehicles as a result of the data, especially personally identifiable data, that these vehicles collect and process in large quantities. Increasingly, the framework also includes laws, regulations, and guidance focused specifically on vehicle autonomy. We begin with a discussion of the regulatory environment in the US, both at the federal and state level, and then turn to non-US jurisdictions, including the EU, China, and Japan.

Regulation in the US

Federal

NHTSA Guidance

The National Highway Traffic Safety Administration (NHTSA) has long been responsible for promulgation and enforcement of the Federal Motor Vehicle Safety Standards. In September 2017, it issued A Vision for Safety 2.0[1], which updated the voluntary guidance for automated and self-driving vehicles released by the Obama administration in September 2016 (the **NHTSA Guidance**). The NHTSA Guidance focuses on the highest levels of vehicle automation, which include systems with no-to-minimal human interaction or performance of driving related tasks. It is divided into two sections. The first offers voluntary guidelines for the autonomous vehicle industry in designing best practices for testing and deployment of autonomous vehicles. The second clarifies federal and state roles in the regulation of autonomous vehicles and provides state legislatures with suggestions for developing best practices on how to safely foster the development and introduction of automated technologies onto public roads.

NHTSA offers suggestions on 12 priority safety design elements [2] to support the industry in developing best practices in the design, development, testing, and deployment of automated vehicle technologies. NHTSA also encourages industry participants to perform voluntary safety self-assessments that demonstrate their approach to testing and deployment. Voluntary safety self-assessments are intended to build public trust in autonomous vehicles and encourage the establishment of industry safety norms. NHTSA envisions that these assessments will also provide information on how the industry is using NHTSA's voluntary guidance or their own processes to address safety concerns. NHTSA's guidance does not require companies to file safety assessments with NHTSA, nor will they need the agency to sign off on a safety assessment prior to testing new autonomous vehicles. Using the assessments, NHTSA has indicated that it plans to regularly update its guidance to reflect lessons learned, new data, and stakeholder input as technology continues to be developed and refined.

SELF DRIVE Act and AV START Act

The House of Representatives passed the SELF DRIVE Act [3] in September 2017 and the Senate passed, by unanimous voice vote, the AV START Act[4] in October 2017. These two acts of Congress respond to calls for regulatory changes at the federal level to promote the development of automated vehicle technology. Both legislative proposals have similar objectives and structures: in general, they seek to preserve the existing regulatory approach to vehicle safety while making modest changes to accommodate self-driving technologies. Both proposals also recognize that longer-term regulatory changes are needed and that more information about the technology will be needed to adopt appropriate longer-term rules. Finally, the proposals both expand federal preemption of state authority over autonomous vehicles by prohibiting state and local governments from legislating in the highly critical areas of design, construction, or performance, thus suggesting that state and local regulations should be focused on traditional state-regulated areas like registration, licensing, insurance, and traffic laws.

While both acts recognize that autonomous vehicles will generate substantial data about vehicle users and their surroundings, they take moderately different approaches to privacy and cybersecurity. The AV START Act arguably goes further than the SELF DRIVE Act in dealing with these concerns:

- The SELF DRIVE Act provides that "A manufacturer may not sell, offer for sale, introduce or deliver for introduction into commerce, or import into the United States," any highly automated vehicle that performs partial driving automation, or automated driving system unless such manufacturer has developed a Privacy Plan[5] and a Cybersecurity Plan[6] that includes written policies and procedures that identify, mitigate, and prevent privacy and cybersecurity vulnerabilities, respectively.
- The AV Start Act would establish a Data Access Advisory Committee to produce a report to Congress with policy recommendations regarding ownership and control of data generated or stored by autonomous vehicles.

The SELF DRIVE Act, in its current form, aims to ensure the safe and innovative development, testing, and deployment of self-driving cars. As noted above, it expressly requires autonomous vehicle manufacturers to develop cybersecurity plans.

The AV START Act is intended to preserve the existing regulatory approach to vehicle safety while making modest changes to accommodate the new technologies. It also requires that manufacturers have a detailed plan [7] for identifying and reducing cybersecurity risks that includes a process for identifying safety-critical control systems, response to and recovery from cyber incidents, information sharing and support of industry standard setting, use of segmentation and isolation techniques in the design of vehicles and systems, and employee training. Finally, the AV START Act allows the Secretary of Transportation to inspect cybersecurity plans to determine whether the manufacturer is in compliance and to work with manufacturers to adopt a coordinated vulnerability disclosure policy.

Other Significant Federal Regulation

There are other federal authorities and rules that impact the development and eventual deployment of autonomous vehicles. The Acting Federal Trade Commission (FTC) Chairman Maureen Ohlhausen [8] made it clear that she expects the FTC's enforcement role in protecting privacy and security to encompass autonomous vehicles and that the FTC would take action against manufacturers and service providers if their activities violate Section 5 of the FTC Act.[9] Section 5 of the FTC Act gives the FTC broad authority to investigate "unfair and deceptive acts and practices in or affecting commerce." The FTC has increasingly used this broad authority aggressively in the privacy and data security contexts, initiating investigations pertaining to a wide variety of alleged "unfair" or "deceptive" practices. This authority was affirmed by the Third Circuit, who upheld a ruling that the FTC could use the prohibition on unfair practices in Section 5 to challenge unreasonable data security practices.[10]

Chairman Ohlhausen also noted that the FTC wants to coordinate its regulatory efforts with the NHTSA. The FTC staff issued a Staff Perspective [11] that outlines their key takeaways from a NHTSA hosted workshop that examined consumer privacy and security issues posed by autonomous vehicles. The FTC staff noted that connected and autonomous cars will have cybersecurity risks that could potentially be exploited by hackers. Developing best practices to address these issues and other consumer privacy concerns will be critical to consumer acceptance and the adopting of the emerging technologies behind connected cars. The FTC staff touted the work of industry initiatives, such as the Consumer Privacy Principles[12] jointly introduced by the Alliance of Automobile Manufacturers and Global Automakers in 2014, as well as the consumer education materials [13] produced by the National Automobile Dealers Association in partnership with the Future of Privacy Forum.

Specific federal legislation, or even laws at the state level (which we discuss below), may be slow to develop given the dynamic technology and the many stakeholders who have an interest in the outcome. Until then, the broad mandate of Section 5 may be one of the main sources of enforcement.

State Regulation

State Regulation Specific to Autonomous Vehicles

State legislatures are becoming increasingly engaged on the topic of autonomous vehicles and are considering how to best regulate in the area. In 2011, Nevada became the first state to authorize the testing of autonomous vehicles on public roads.[14] Since then, more than half the states have either passed legislation or issued executive orders that allow for or regulate the use or function of autonomous vehicles.[15]

California's autonomous vehicle statute[16] was signed into law in September 2012 and permits the operation of autonomous vehicles on California roads under certain conditions. One condition requires the autonomous vehicle to have a separate mechanism that captures and stores the vehicle's sensor data for at least 30 seconds before a collision occurs. The statute states that the 30-second clips must be preserved for three years after the date of a collision. The statute also requires that the vehicle's technology meet the Federal Motor Vehicle Safety Standards for the vehicle's model and year. Since its 2012 law, California authorized the Contra Costa Transportation Authority to conduct a pilot project that allows for the testing fully autonomous vehicles that are not equipped with a steering wheel, brake pedal, or accelerator.[17] The law mandates that all testing would be conducted at a privately owned business park or the former Concord Naval Weapons Station and requires the autonomous vehicles travel at a speed of 35 miles per hour or less.

Michigan enacted a series of laws[18] in 2016 that authorize further testing and use of autonomous vehicles on all public roads within the state. Notably, the laws are one of the first to permit the operation of autonomous vehicles without a

driver behind the wheel on public roads. Under those laws, the automated driving system is recognized to be the driver or operator of the autonomous vehicle for purposes of determining compliance with traffic laws. The laws also allow for ride-sharing services without drivers to be operated by vehicle manufacturers or ride-hailing services such as Uber or Lyft.

Florida followed in Michigan's footsteps in 2016 by amending its 2012 law to allow for the operation of autonomous vehicles on public roads without a driver physically present in the vehicle.[19] The amended statute allows any individual who possesses a valid driver's license to operate an autonomous vehicle so long as the autonomous vehicle can alert the operator of a technology failure and be capable of bringing itself to a complete stop. It does not require any additional special training or driver education. However, the vehicle must be registered and meet the applicable federal safety standards and regulations. The 2016 amendments also stripped away key restrictions from Florida's 2012 law. For instance, entities testing autonomous vehicles on Florida's roads are no longer required to carry $5 million in insurance coverage. Additionally, Florida's traffic laws prohibit individuals sitting in the driver's seat from viewing entertainment content while the vehicle is in motion; however, the 2016 statute provides an exception to this long-standing rule for self-driving vehicles operated in autonomous mode.

State Regulation with Implications for Autonomous and Connected Vehicles

Although not every state has contemplated or adopted laws related to autonomous vehicles, most states have laws requiring reasonable security, data storage, and data retention with respect to certain types of data, especially personally identifiable information of the sort that will be generated in huge volumes by autonomous vehicles. For instance, California[20] has a relevant and illustrative law that requires businesses to implement reasonable security procedures to protect personal information from unauthorized access, use, destruction, modification or disclosure. In addition, the California Attorney General issued a report in 2016 stating that the Center for Internet Security Critical Security Controls (CIS Controls)[21] represent a minimum level of security that all companies should maintain. All of these controls are potentially relevant to companies creating autonomous vehicle technology.

International Regulation

United Kingdom

The United Kingdom has not yet enacted legislation regulating the use of autonomous vehicles. However, in 2017, the UK government announced a plan to introduce the Automated and Electric Vehicles Bill, which pledges £200 million towards inventing, designing, and safely operating autonomous vehicle technology in the UK. Also, in August 2018, the government issued non-binding guidance outlining the UK's goals related to the protection of information obtained through autonomous vehicles. The guidance is called 'The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles' and is aimed at ensuring minimum cybersecurity protections in the manufacture and operation of autonomous vehicles. The guidance outlines eight principles[22], which are articulated at a high level.

Germany

In May 2017, the German Parliament approved legislation allowing for autonomous vehicles to be road-tested so long as a driver was sitting behind the wheel of the vehicle fully capable of taking back control of the vehicle when alerted by the vehicle to do so. Part of the legislation requires the use of a vehicle black box for purposes of recording each drive and logging whether the human or the vehicle was in control of the ride and for which parts.

Additionally, Germany recently adopted the world's first set of ethical guidelines that require autonomous vehicles to prioritize human life over damage to property or animals in the event of an accident. The guidelines mandate that autonomous vehicle software be programed to avoid human injury or death at all costs and prohibit factoring in the age, sex, or physical condition of the person(s) involved.

France

In October 2017, the French Commission Nationale de L'informatique et des Libertés (the CNIL) released a "compliance pack" for connected cars that provides guidance to stakeholders on how to integrate the principle of "privacy by design" into their production pipeline.[23] The compliance pack weaves in principles from French data protection law and the GDPR (as defined below), reminding stakeholders of the importance of transparency and fairness in data collection, and of giving individuals control over their data. The CNIL noted that the compliance pack is an evolving document that will be updated and finalized after the GDPR comes into effect.

European Union

Although not specific to autonomous vehicles, the EU's General Data Protection Regulation (GDPR), which comes into force May 25, 2018, will have an impact on the processing of any personally identifiable data collected from autonomous vehicles. GDPR recognizes a range of rights for EU data subjects and places a number of obligations on the "controllers" and the "processors" of personal data.

The implications for the manufacturers, suppliers, drivers, and any other party that takes part in the supply chain of autonomous vehicles are considerable. For example, GDPR will require considerable effort to collect only that data which is essential to autonomous driving while balancing and respecting the privacy rights of the data subjects about whom that data relates. This may mean, for example, that the collectors of images taken by the systems of autonomous vehicles (*e.g.*, images of the environment and surroundings) may need to anonymize such data so that it cannot be used to identify any specific individual. It may also mean that autonomous vehicle companies need to incorporate "privacy by design" principles into their hardware and software so they can enable data subjects or other third parties to access and modify data in accordance with their rights under GDPR.

Critically, GDPR shifts the burden of proof as to compliance, meaning that autonomous vehicle companies will need to be able to prove that they comply with GDPR. This will be exceptionally difficult because of the nature of the autonomous vehicles' continuous data streams that capture large volumes of data that need to be maintained for various amounts of time. For evidence of accountability, companies will likely need to maintain detailed records showing how the personal data was collected and processed consistent with GDPR's requirements. In addition, stakeholders across the autonomous vehicle supply chain will be responsible for this data and will need to enter into carefully structured agreements that clearly identify each party's respective obligations with respect to the use and protection of the data and the apportionment of risk if that data is compromised.

Japan

The Japanese government is in the initial stages of creating national regulation supporting the use of autonomous vehicles. In May 2016, Japan's National Police Agency adopted approval standards for testing autonomous vehicles on its roadways. A portion of the standards focuses on developing data from the autonomous vehicle trials for purposes of protecting autonomous vehicles from cyberattacks.

China

China also has been active in this space. China recently enacted a Network Security Law (also known as its Cybersecurity Law) that provides a basis for new laws and regulations in this area. The law requires network operators in critical infrastructure sectors, which include transportation and in turn autonomous vehicles, to store within China the data that is gathered or produced there. Of particular note, Article 21 of the Network Security Law imposes an obligation to adopt "technical measures for monitoring and recording network operation status and the network security incidents" and to keep "relevant network logs for at least 6 months." Again, this will impose significant data storage requirements with respect to autonomous vehicles.

China's Network Security Law took effect on June 1, 2017. The law applies to network operators and businesses in critical sectors, which includes transportation. The law requires network operators to coordinate with Chinese investigators and subjects them to additional regulation in areas such as the protection of personal information, critical infrastructure information, and preservation of sensitive information. Importantly, the law requires network operators in critical sectors to store within mainland China data that is gathered or produced by the network operator in the country. In ambiguous terms, the law also requires network operators to "obey social norms and commercial ethics, be honest and credible, perform obligations to protect network security, accept supervision from the government and public, and bear social responsibility." The contours of the law are still being understood, but it is clear that many businesses operating internet of things infrastructure in China will be considered "network operators" subject to additional regulation.

China is also limiting the amount of mapping of roads that can be done by foreign companies, making it significantly more difficult for foreign car makers to produce autonomous vehicles for China, which rely on mapping for navigation. Only 13 Chinese companies are licensed by the government for surveying and mapping. Foreign car companies are contracting with these particular companies.

Australia

The Australian government is currently considering how to effectively regulate the use of autonomous vehicles, as it acknowledges that autonomous vehicles could have a heavy presence on Australian roads as early as 2020. The National Transportation Commission of Australia (NTC) already identified over 700 laws, rules, and regulations that will require revision in order to support the wave of autonomous vehicle usage, but no changes have yet been made.

In May 2017, the NTC published and the Australian travel ministers approved guidelines related to testing of autonomous vehicles. Under these guidelines, the NTC plans to develop a safety assurance regime for autonomous vehicles and create guidelines for clarifying regulatory concepts of proper control for different levels of automation by November 2017. The NTC also plans to curate legislative reform efforts to clarify current laws and establish legal obligations for automated driving systems by May 2018. Finally, the NTC guidelines include plans to create options for managing government access to data created by automated vehicles and to support jurisdiction-based legislation related to on-road driving trials and to reviewing insurance schemes.

Conclusion

Although the regulatory framework for autonomous vehicles is developing rapidly, many of the regulations and guidance documents are limited in scope. This reflects the difficulties of trying to regulate in an area where the technology is evolving at such a rapid pace, but it also likely reflects concern about the risk that strict regulation might result in the migration of autonomous vehicle development programs, and the jobs that go with them, to less stringent jurisdictions. For companies in the autonomous vehicle space, it will be important to track developments on the regulatory front in all applicable jurisdictions and to ensure that reasonable steps are taken in all key phases of the development, testing, and roll-out of autonomous vehicles. These steps would include a robust cybersecurity and privacy program that complies with all applicable laws as well as thoughtful contracting practices that mitigate cybersecurity and privacy risks across the supply chain. On the privacy front, companies will need to consider key privacy principles that are embodied in various laws around the world, including principles relating to data minimization, purpose limitation, and notice and consent.

---

[1] NHTSA, A Vision for Safety 2.0, available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf. See also McDermott Will & Emery, The Department of Transportation Helps Clear the Road for Autonomous Vehicles, available at https://www.mwe.com/en/thought-leadership/publications/2017/09/department-transportation-road-autonomous-vehicles.

[2] The 12 priority safety design elements include: (1) System Safety: NHTSA encourages industry to adopt and follow standards in safety, including those from standards-developing organizations, and to document the safety design process; (2) Operational Design Domain (ODD): NHTSA encourages industry to define the ODD for each vehicle's automated driving system and document the assessment, testing, and validation procedure. An ODD defines where (such as roadways types and speeds) and when (day/night, weather limits, etc.) an autonomous vehicle is designed to operate; (3) Object and Event Detection and Response (OEDR): OEDR refers to detection of unexpected circumstances relevant to driving, such as pedestrians, bicyclists, animals, and objects. NHTSA encourages industry to have a documented process for assessment, testing, and validation of OEDR capabilities, (4) Fallback: NHTSA encourages industry to have a documented process for transitioning to a "minimal risk condition" where it cannot do any harm when a problem is encountered or the vehicle cannot operate safely; (5) Validation Methods: Given the variety of automation functions, NHTSA encourages industry to develop methods to mitigate safety risks associated with their automated approach. Industry should continue to work with NHTSA and standards organizations to develop and update safety tests; (6) Human Machine Interface: NHTSA encourages industry to consider whether driver engagement monitoring is necessary. An autonomous vehicle should be capable of informing the human operator or occupant whether the vehicle is properly functioning; (7) Vehicle Cybersecurity: NHTSA encourages industry to follow established best practices and design principles for cyber security and to consider and incorporate guidance from a variety of standards setting organizations; (8) Crashworthiness: NHTSA encourages industry to consider how best to protect vehicle occupants and to include information from advanced sensing technologies into new occupant protection systems; (9) Post-Crash Behavior: NHTSA encourages industry to consider methods of returning an automated vehicle to a safe state after being involved in a crash, such as shutting off the fuel pump and disengaging electrical power; (10) Data Recording: NHTSA encourages industry to establish a process for testing, validating, and collecting data related to malfunctions, degradations, or failures. Data gathered from crashes should be used to update standards as well as for crash reconstruction purposes; (11) Consumer Education and Training: NHTSA encourages industry to develop dealer, distributor, and consumer education and training programs on the safe use and operation of autonomous vehicles; and (12) Federal, State, and Local Laws: NHTSA encourages industry to document how they intend to account for all applicable federal, state, and local laws in the design of their vehicles and automated driving systems.

[3] The SELF DRIVE Act, H.R. 3388 (September 7, 2017).

[4] The AV START Act, S. 1885 (September 28, 2017).

[5] The SELF DRIVE Act requires a manufacturer's privacy plan to include: (1) A written privacy plan with respect to the collection, use, sharing, and storage or information about vehicle owners or occupants collected by the vehicle. That written policy must include (a) the practices with respect to the way that information is collected, used, shared, and stored; (b) the practices with respect to the choices offered to vehicle owners and occupants regarding the collection, use, sharing, and storage of such information; (c) the practices with respect to data minimization, de-identification, and retention of information; and (d) the practices with respect to extending its privacy plan to with whom entities it shares such information; and (2) a method for providing notice to vehicle owners or occupants about the privacy policy.

[6] The SELF DRIVE Act requires a manufacturer's cybersecurity plan to include: (1) A written cybersecurity policy outlining the manufacturer's practices for detecting and responding to cyber-attacks, unauthorized intrusions, and false and spurious messages or vehicle control commands. That written policy must include (a) a process for identifying, assessing, and mitigating reasonably foreseeable vulnerabilities from cyber-attacks; and (b) a process for taking preventative and corrective action to mitigate against vulnerabilities in highly automated vehicles or vehicles that perform partial driving automation; (2) Identification of an officer of the manufacturer responsible for management of cybersecurity; (3) A process for limiting access to automated driving systems; and (4) A process for employee training and supervision for implementation and maintenance of the policies, including controls on employee access to automated driving systems.
[7] Specifically, the AV START Act cybersecurity plan must include processes for: (1) Risk-based prioritized identification and protection of safety-critical vehicle control systems and the broader transportation ecosystem; (2) Efficient detection and response to potential cybersecurity incidents in the field; (3) Facilitating expeditious recovery from incidents as they occur; (4) The institutionalization of methods for accelerated adoption of lessons learned across industry through voluntary exchange of information related to cybersecurity; (5) Identification of the point of contact at a manufacturer responsible for management of cybersecurity; (6) Use of segmentation and isolation techniques in vehicle design; and (7) Supporting voluntary efforts by industry and standards-setting organizations to develop and identify consistent cybersecurity standards relating to vehicles.
[8] Remarks from the FTC Connected Cars Workshop, June 28, 2017, available at https://www.ftc.gov/public-statements/2017/06/remarks-ftc-connected-cars-workshop.
[9] The FTC Act, 15 U.S.C. Sec. 45(a)(1).
[10] FTC v. Wyndham Worldwide Corporation, 799 F.3d 236 (3d Cir. 2015).
[11] FTC Staff Perspective, Connected Cars Workshop, January 2018, available at https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf.
[12] Alliance of Automobile Manufacturers, Inc. and Association for Global Automakers, Inc., Consumer Privacy Protection Principles, Privacy Principles for Vehicle Technologies and Services, November 12, 2014, available at https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf.
[13] See, *e.g.*, National Automobile Dealers Association and the Future of Privacy Forum, Personal Data in your Car, available at https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf.
[14] See Nev. Rev. Stat. § 484B (2011).
[15] As of December 2017, 21 state legislatures enacted laws related to autonomous vehicles and 5 governors issued executive orders. The 21 states to enact laws are Alabama, Arkansas, California, Connecticut, Florida, Georgia, Illinois, Louisiana, Michigan, New York, Nevada, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Vermont, and Virginia. The District of Columbia also enacted legislation regulating the use of autonomous vehicles. The five governors to issue executive orders are from Arizona, Delaware, Massachusetts, Washington, and Wisconsin.
[16] Cal. Veh. Code § 38750 (2012).
[17] Cal. Veh. Code § 38755 (2016).
[18] Michigan SB §§ 995-998 (2016).
[19] Fla. House Bill 7027 (2016) (approved by Florida Governor on April 4, 2016 and enacted on July 1, 2016). In 2012, Florida enacted its first law regulating the usage and testing of autonomous vehicles. The 2012 law allowed for the testing of autonomous vehicles on Florida's public roads, but required that the operator of the vehicle remain present in the vehicle so as to monitor the vehicle's performance and intervene as necessary. It also restricted those persons qualified to operate an autonomous vehicle on Florida's public roads to "employees, contractors, or other persons designed by manufacturers of autonomous technology for the purpose of testing the technology." Fla. House Bill 1207.5(1) (2012) (enacted on April 16, 2012).
[20] Cal. Civ. Code § 1798.81.5 (2014).
[21] Center for Internet Security Critical Security Controls, available at https://www.cisecurity.org/controls/.
[22] The eight principles of 'The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles are as follows: Principle 1 – Organization 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; Principle 3 – Organizations need product aftercare and incident response to ensure systems are secure over their lifetime; Principle 4 – All organizations, including subcontractors, supplies, 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; and Principle 8 – The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail.
[23] CNIL, Connected Vehicles: A Compliance Pack for Responsible Data Use, October 17, 2017, available at https://www.cnil.fr/fr/vehicules-connectes-un-pack-de-conformite-pour-une-utilisation-responsable-des-donnees (in French).

The material in this publication may not be reproduced, in whole or part without acknowledgement of its source and copyright. A Short Primer on Autonomous and Connected Vehicle Regulation is intended to provide information of general interest in a summary manner and should not be construed as individual legal advice. Readers should consult with their McDermott Will & Emery lawyer or other professional counsel before acting on the information contained in this publication.

©2018 McDermott Will & Emery. The following legal entities are collectively referred to as "McDermott Will & Emery," "McDermott" or "the Firm": McDermott Will & Emery LLP, McDermott Will & Emery AARPI, McDermott Will & Emery Belgium LLP, McDermott Will & Emery Rechtsanwälte Steuerberater LLP, McDermott Will & Emery Studio Legale Associato and McDermott Will & Emery UK LLP. These entities coordinate their activities through service agreements. McDermott has a strategic alliance with MWE China Law Offices, a separate law firm. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome

Office Locations

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9-31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
227 West Monroe Street
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: + 49 69 271599 633

HOUSTON
1000 Louisiana Street, Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
Heron Tower
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East, 38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas, Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza, Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road, Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, DC
The McDermott Building
500 North Capitol Street, NW
Washington, DC 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087

Boston Brussels Chicago
Düsseldorf Frankfurt Houston London
Los Angeles Miami Milan Munich
New York Orange County Paris
Seoul Silicon Valley Washington, DC

Strategic alliance with MWE China Law Offices
(Shanghai)

www.mwe.com