GIBSON DUNN

October 10, 2018

ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS LEGAL UPDATE (3Q18)

To Our Clients and Friends:

We are pleased to provide the following update on recent legal developments in the areas of artificial intelligence, machine learning, and autonomous systems (or "AI" for short), and their implications for companies developing or using products based on these technologies. As the spread of AI rapidly increases, legal scrutiny in the U.S. of the potential uses and effects of these technologies (both beneficial and harmful) has also been increasing. While we have chosen to highlight below several governmental and legislative actions from the past quarter, the area is rapidly evolving and we will continue to monitor further actions in these and related areas to provide future updates of potential interest on a regular basis.

I. Increasing Federal Government Interest in AI Technologies

The Trump Administration and Congress have recently taken a number of steps aimed at pushing AI forward on the U.S. agenda, while also treating with caution foreign involvement in U.S.-based AI technologies. Some of these actions may mean additional hurdles for cross-border transactions involving AI technology. On the other hand, there may also be opportunities for companies engaged in the pursuit of AI technologies to influence the direction of future legislation at an early stage.

A. White House Studies AI

In May, the Trump Administration kicked off what is becoming an active year in AI for the federal government by hosting an "Artificial Intelligence for American Industry" summit as part of its designation of AI as an "Administration R&D priority."[1] During the summit, the White House also announced the establishment of a "Select Committee on Artificial Intelligence" to advise the President on research and development priorities and explore partnerships within the government and with industry.[2] This Select Committee is housed within the National Science and Technology Council, and is chaired by Office of Science and Technology Policy leadership.

Administration officials have said that a focus of the Select Committee will be to look at opportunities for increasing federal funds into AI research in the private sector, to ensure that the U.S. has (or maintains) a technological advantage in AI over other countries. In addition, the Committee is to look at possible uses of the government's vast store of taxpayer-funded data to promote the development of advanced AI technologies, without compromising security or individual privacy. While it is believed that there will be opportunities for private stakeholders to have input into the Select Committee's deliberations, the inaugural meeting of the Committee, which occurred in late June, was not open to the public for input.

B. AI in the NDAA for 2019

More recently, on August 13th, President Trump signed into law the John S. McCain National Defense Authorization Act (NDAA) for 2019,[3] which specifically authorizes the Department of Defense to appoint a senior official to coordinate activities relating to the development of AI technologies for the military, as well as to create a strategic plan for incorporating a number of AI technologies into its defense arsenal. In addition, the NDAA includes the Foreign Investment Risk Review Modernization Act (FIRRMA)[4] and the Export Control Reform Act (ECRA),[5] both of which require the government to scrutinize cross-border transactions involving certain new technologies, likely including AI-related technologies.

FIRRMA modifies the review process currently used by the Committee on Foreign Investment in the United States (CFIUS), an interagency committee that reviews the national security implications of investments by foreign entities in the United States. With FIRRMA's enactment, the scope of the transactions that CFIUS can review is expanded to include those involving "emerging and foundational technologies," defined as those that are critical for maintaining the national security technological advantage of the United States. While the changes to the CFIUS process are still fresh and untested, increased scrutiny under FIRRMA will likely have an impact on available foreign investment in the development and use of AI, at least where the AI technology involved is deemed such a critical technology and is sought to be purchased or licensed by foreign investors.

Similarly, ECRA requires the President to establish an interagency review process with various agencies including the Departments of Defense, Energy, State and the head of other agencies "as appropriate," to identify emerging and foundational technologies essential to national security in order to impose appropriate export controls. Export licenses are to be denied if the proposed export would have a "significant negative impact" on the U.S. defense industrial base. The terms "emerging and foundational technologies" are not expressly defined, but it is likely that AI technologies, which are of course "emerging," would receive a close look under ECRA and that ECRA might also curtail whether certain AI technologies can be sold or licensed to foreign entities.

The NDAA also established a National Security Commission on Artificial Intelligence "to review advances in artificial intelligence, related machine learning developments, and associated technologies." The Commission, made up of certain senior members of Congress as well as the Secretaries of Defense and Commerce, will function independently from other such panels established by the Trump Administration and will review developments in AI along with assessing risks related to AI and related technologies to consider how those methods relate to the national security and defense needs of the United States. The Commission will focus on technologies that provide the U.S. with a competitive AI advantage, and will look at the need for AI research and investment as well as consider the legal and ethical risks associated with the use of AI. Members are to be appointed within 90 days of the Commission being established and an initial report to the President and Congress is to be submitted by early February 2019.

C. Additional Congressional Interest in AI/Automation

While a number of existing bills with potential impacts on the development of AI technologies remain stalled in Congress,[6] two more recently-introduced pieces of legislation are also worth monitoring as they progress through the legislative process.

In late June, Senator Feinstein (D-CA) sponsored the "Bot Disclosure and Accountability Act of 2018," which is intended to address some of the concerns over the use of automated systems for distributing content through social media.[7] As introduced, the bill seeks to prohibit certain types of bot or other automated activity directed to political advertising, at least where such automated activity appears to impersonate human activity. The bill would also require the Federal Trade Commission to establish and enforce regulations to require public disclosure of the use of bots, defined as any "automated software program or process intended to impersonate or replicate human activity online." The bill provides that any such regulations are to be aimed at the "social media provider," and would place the burden of compliance on such providers of social media websites and other outlets. Specifically, the FTC is to promulgate regulations requiring the provider to take steps to ensure that any users of a social media website owned or operated by the provider would receive "clear and conspicuous notice" of the use of bots and similar automated systems. FTC regulations would also require social media providers to police their systems, removing non-compliant postings and/or taking other actions (including suspension or removal) against users that violate such regulations. While there are significant differences, the Feinstein bill is nevertheless similar in many ways to California's recently-enacted Bot disclosure law (S.B. 1001), discussed more fully in our previous client alert located here.[8]

Also of note, on September 26th, a bipartisan group of Senators introduced the "Artificial Intelligence in Government Act," which seeks to provide the federal government with additional resources to incorporate AI technologies in the government's operations.[9] As written, this new bill would require the General Services Administration to bring on technical experts to advise other government agencies, conduct research into future federal AI policy, and promote inter-agency cooperation with regard to AI technologies. The bill would also create yet another federal advisory board to advise government agencies on AI policy opportunities and concerns. In addition, the newly-introduced legislation seeks to require the Office of Management and Budget to identify ways for the federal government to invest in and utilize AI technologies and tasks the Office of Personal Management with anticipating and providing training for the skills and competencies the government requires going-forward for incorporating AI into its overall data strategy.

II. Potential Impact on AI Technology of Recent California Privacy Legislation

Interestingly, in the related area of data privacy regulation, the federal government has been slower to respond, and it is the state legislatures that are leading the charge.[10]

Most machine learning algorithms depend on the availability of large data sets for purpose of training, testing, and refinement. Typically, the larger and more complete the datasets available, the better. However, these datasets often include highly personal information about consumers, patients, or

others of interest—data that can sometimes be used to predict information specific to a particular person even if attempts are made to keep the source of such data anonymous.

The European Union's General Data Protection Regulation, or GDPR, which went into force on May 25, 2018, has deservedly garnered a great deal of press as one of the first, most comprehensive collections of data privacy protections. While we're only months into its effective period, the full impact and enforcement of the GDPR's provisions have yet to be felt. Still, many U.S. companies, forced to take steps to comply with the provisions of GDPR at least with regard to EU citizens, have opted to take many of those same steps here in the U.S., despite the fact that no direct U.S. federal analogue to the GDPR yet exists.[11]

Rather than wait for the federal government to act, several states have opted to follow the lead of the GDPR and enact their own versions of comprehensive data privacy laws. Perhaps the most significant of these state-legislated omnibus privacy laws is the California Consumer Privacy Act ("CCPA"), signed into law on June 28, 2108, and slated to take effect on January 1, 2020.[12] The CCPA is not identical to the GDPR, differing in a number of key respects. However there are many similarities, in that the CCPA also has broadly defined definitions of personal information/data, and seeks to provide a right to notice of data collection, a right of access to and correction of collected data, a right to be forgotten, and a right to data portability. But how do the CCPA's requirements differ from the GDPR for companies engaged in the development and use of AI technologies? While there are many issues to consider, below we examine several of the key differences of the CCPA and their impact on machine learning and other AI-based processing of collected data.

A. Inferences Drawn from Personal Information

The GDPR defines personal data as "any information relating to an identified or identifiable natural person," such as "a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that nature person."[13] Under the GDPR, personal data has implications in the AI space beyond just the data that is actually collected from an individual. AI technology can be and often is used to generate additional information about a person from collected data, e.g., spending habits, facial features, risk of disease, or other inferences that can be made from the collected data. Such inferences, or derivative data, may well constitute "personal data" under a broad view of the GDPR, although there is no specific mention of derivative data in the definition.

By contrast, the CCPA goes farther and specifically includes "inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes."[14] An "inference" is defined as "the derivation of information, data, assumptions, or conclusions from evidence, or another source of information or data."[15]

Arguably the primary purpose of many AI systems is to draw inferences from a user's information, by mining data, looking for patterns, and generating analysis. Although the CCPA does limit inferences to those drawn "to create a profile about a consumer," the term "profile" is not defined in the

CCPA. However, the use of consumer information that is "deidentified" or "aggregated" is permitted by the CCPA. Thus, one possible solution may be to take steps to "anonymize" any personal data used to derive any inferences. As a result, when looking to CCPA compliance, companies may want to carefully consider the derivative/processed data that they are storing about a user, and consider additional steps that may be required for CCPA compliance.

B. Identifying Categories of Personal Information

The CCPA also requires disclosures of the categories of personal information being collected, the categories of sources from which personal information is collected, the purpose for collecting and selling personal information, and the categories of third parties with whom the business shares personal information. [16] Although these categories are likely known and definable for static data collection, it may be more difficult to specifically disclose the purpose and categories for certain information when dynamic machine learning algorithms are used. This is particularly true when, as discussed above, inferences about a user are included as personal information. In order to meet these disclosure requirements, companies may need to carefully consider how they will define all of the categories of personal information collected or the purposes of use of that information, particularly when machine learning algorithms are used to generate additional inferences from, or derivatives of, personal data.

C. Personal Data Includes Households

The CCPA's definition of "personal data" also includes information pertaining to non-individuals, such as "households" – a term that the CCPA does not further define.[17] In the absence of an explicit definition, the term "household" would seem to target information collected about a home and its inhabits through smart home devices, such as thermostats, cameras, lights, TVs, and so on. When looking to the types of personal data being collected, the CCPA may also encompass information about each of these smart home devices, such as name, location, usage, and special instructions (e.g., temperature controls, light timers, and motion sensing). Furthermore, any inferences or derivative information generated by AI algorithms from the information collected from these smart home devices may also be covered as personal information. Arguably, this could include information such as conversations with voice assistants or even information about when people are likely to be home determined via cameras or motion sensors. Companies developing smart home, or other Internet of Things, devices thus should carefully consider whether the scope and use they make of any information collected from "households" falls under the CCPA requirements for disclosure or other restrictions.

III. Continuing Efforts to Regulate Autonomous Vehicles

Much like the potential for a comprehensive U.S. data privacy law, and despite a flurry of legislative activity in Congress in 2017 and early 2018 towards such a national regulatory framework, autonomous vehicles continue to operate under a complex patchwork of state and local rules with limited federal oversight. We previously provided an update (located here)[18] discussing the Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution (SELF DRIVE) Act[19], which passed the U.S. House of Representatives by voice vote in September 2017 and its companion bill (the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START)

Act).[20] Both bills have since stalled in the Senate, and with them the anticipated implementation of a uniform regulatory framework for the development, testing and deployment of autonomous vehicles.

As the two bills languish in Congress, 'chaperoned' autonomous vehicles have already begun coexisting on roads alongside human drivers. The accelerating pace of policy proposals—and debate surrounding them—looks set to continue in late 2018 as virtually every major automaker is placing more autonomous vehicles on the road for testing and some manufacturers prepare to launch commercial services such as self-driving taxi ride-shares[21] into a national regulatory vacuum.

A. "Light-touch" Regulation

The delineation of federal and state regulatory authority has emerged as a key issue because autonomous vehicles do not fit neatly into the existing regulatory structure. One of the key aspects of the proposed federal legislation is that it empowers the National Highway Traffic Safety Administration (NHTSA) with the oversight of manufacturers of self-driving cars through enactment of future rules and regulations that will set the standards for safety and govern areas of privacy and cybersecurity relating to such vehicles. The intention is to have a single body (the NHTSA) develop a consistent set of rules and regulations for manufacturers, rather than continuing to allow the states to adopt a web of potentially widely differing rules and regulations that may ultimately inhibit development and deployment of autonomous vehicles. This approach was echoed by safety guidelines released by the Department of Transportation (DoT) for autonomous vehicles. Through the guidelines ("a nonregulatory approach to automated vehicle technology safety"),[22] the DoT avoids any compliance requirement or enforcement mechanism, at least for the time being, as the scope of the guidance is expressly to support the industry as it develops best practices in the design, development, testing, and deployment of automated vehicle technologies. Under the proposed federal legislation, the states can still regulate autonomous vehicles, but the guidance encourages states not to pass laws that would "place unnecessary burdens on competition and innovation by limiting [autonomous vehicle] testing or deployment to motor vehicle manufacturers only."[23] The third iteration of the DoT's federal guidance, published on October 4, 2018, builds upon—but does not replace—the existing guidance, and reiterates that the federal government is placing the onus for safety on companies developing the technologies rather than on government regulation. [24] The guidelines, which now include buses, transit and trucks in addition to cars, remain voluntary.

B. Safety

Much of the delay in enacting a regulatory framework is a result of policymakers' struggle to balance the industry's desire to speed both the development and deployment of autonomous vehicle technologies with the safety and security concerns of consumer advocates.

The AV START bill requires that NHTSA must construct comprehensive safety regulations for AVs with a mandated, accelerated timeline for rulemaking, and the bill puts in place an interim regulatory framework that requires manufacturers to submit a Safety Evaluation Report addressing a range of key areas at least 90 days before testing, selling, or commercialization of an driverless cars. But some lawmakers and consumer advocates remain skeptical in the wake of highly publicized setbacks in

autonomous vehicle testing.[25] Although the National Safety Transportation Board (NSTB) has authority to investigate auto accidents, there is still no federal regulatory framework governing liability for individuals and states.[26] There are also ongoing concerns over cybersecurity risks[27], the use of forced arbitration clauses by autonomous vehicle manufacturers,[28] and miscellaneous engineering problems that revolve around the way in which autonomous vehicles interact with obstacles commonly faced by human drivers, such as emergency vehicles,[29] graffiti on road signs or even raindrops and tree shadows.[30]

In August 2018, the Governors Highway Safety Association (GHSA) published a report outlining the key questions that manufacturers should urgently address.[31] The report suggested that states seek to encourage "responsible" autonomous car testing and deployment while protecting public safety and that lawmakers "review all traffic laws." The report also notes that public debate often blurs the boundaries between the different levels of automation the NHTSA has defined (ranging from level 0 (no automation) to level 5 (fully self-driving without the need for human occupants)), remarking that "most AVs for the foreseeable future will be Levels 2 through 4. Perhaps they should be called 'occasionally self-driving.'"[32]

C. State Laws

Currently, 21 states and the District of Columbia have passed laws regulating the deployment and testing of self-driving cars, and governors in 10 states have issued executive orders related to them.[33] For example, California expanded its testing rules in April 2018 to allow for remote monitoring instead of a safety driver inside the vehicle.[34] However, state laws differ on basic terminology, such as the definition of "vehicle operator." Tennessee SB 151[35] points to the autonomous driving system (ADS) while Texas SB 2205[36] designates a "natural person" riding in the vehicle. Meanwhile, Georgia SB 219[37] identifies the operator as the person who causes the ADS to engage, which might happen remotely in a vehicle fleet. These distinctions will affect how states license both human drivers and autonomous vehicles going forward. Companies operating in this space accordingly need to stay abreast of legal developments in states in which they are developing or testing autonomous vehicles, while understanding that any new federal regulations may ultimately preempt those states' authorities to determine, for example, crash protocols or how they handle their passengers' data.

D. 'Rest of the World'

While the U.S. was the first country to legislate for the testing of automated vehicles on public roads, the absence of a national regulatory framework risks impeding innovation and development. In the meantime, other countries are vying for pole position among manufacturers looking to test vehicles on roads.[38] KPMG's 2018 Autonomous Vehicles Readiness Index ranks 20 countries' preparedness for an autonomous vehicle future. The Netherlands took the top spot, outperforming the U.S. (3rd) and China (16th).[39] Japan and Australia plan to have self-driving cars on public roads by 2020.[40] The U.K. government has announced that it expects to see fully autonomous vehicles on U.K. roads by 2021, and is introducing legislation—the Automated and Electric Vehicles Act 2018—which installs an insurance framework addressing product liability issues arising out of accidents involving autonomous cars, including those wholly caused by an autonomous vehicle "when driving itself."[41]

E. Looking Ahead

While autonomous vehicles operating on public roads are likely to remain subject to both federal and state regulation, the federal government is facing increasing pressure to adopt a federal regulatory scheme for autonomous vehicles in 2018.[42] Almost exactly one year after the House passed the SELF DRIVE Act, House Energy and Commerce Committee leaders called on the Senate to advance automated vehicle legislation, stating that "[a]fter a year of delays, forcing automakers and innovators to develop in a state-by-state patchwork of rules, the Senate must act to support this critical safety innovation and secure America's place as a global leader in technology."[43] The continued absence of federal regulation renders the DoT's informal guidance increasingly important. The DoT has indicated that it will enact "flexible and technology-neutral" policies—rather than prescriptive performance-based standards—to encourage regulatory harmony and consistency as well as competition and innovation.[44] Companies searching for more tangible guidance on safety standards at federal level may find it useful to review the recent guidance issued alongside the DoT's announcement that it is developing (and seeking public input into) a pilot program for 'highly or fully' autonomous vehicles on U.S. roads.[45] The safety standards being considered include technology disabling the vehicle if a sensor fails or barring vehicles from traveling above safe speeds, as well as a requirement that NHTSA be notified of any accident within 24 hours.

---

[1] *See* https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf; note also that the Trump Administration's efforts in studying AI technologies follow, but appear largely separate from, several workshops on AI held by the Obama Administration in 2016, which resulted in two reports issued in late 2016 (*see* *Preparing for the Future of Artificial Intelligence*, and *Artificial Intelligence, Automation, and the Economy*).

[2] *Id.* at Appendix A.

[3] *See* https://www.mccain.senate.gov/public/index.cfm/2018/8/senate-passes-the-john-s-mccain-national-defense-authorization-act-for-fiscal-year-2019. The full text of the NDAA is available at https://www.congress.gov/bill/115th-congress/house-bill/5515/text. For additional information on CFIUS reform implemented by the NDAA, please see Gibson Dunn's previous client update at https://www.gibsondunn.com/cfius-reform-our-analysis/.

[4] *See id.*; *see also* https://www.treasury.gov/resource-center/international/Documents/FIRRMA-FAQs.pdf.

[5] *See* https://foreignaffairs.house.gov/wp-content/uploads/2018/02/HR-5040-Section-by-Section.pdf.

[6] *See, e.g. infra.*, Section III discussion of SELF DRIVE and AV START Acts, among others.

[7] S.3127, 115th Congress (2018).

[8] https://www.gibsondunn.com/new-california-security-of-connected-devices-law-and-ccpa-amendments/.

[9] S.3502, 115th Congress (2018).

[10] *See also, infra.*, Section III for more discussion of specific regulatory efforts for autonomous vehicles.

[11] However, as 2018 has already seen a fair number of hearings before Congress relating to digital data privacy issues, including appearances by key executives from many major tech companies, it seems likely that it may not be long before we see the introduction of a "GDPR-like" comprehensive data privacy bill. Whether any resulting federal legislation would actually pre-empt state-enacted privacy laws to establish a unified federal framework is itself a hotly-contested issue, and remains to be seen.

[12] AB 375 (2018); Cal. Civ. Code §1798.100, *et seq.*

[13] Regulation (EU) 2016/679 (General Data Protection Regulation), Article 4 (1).

[14] Cal. Civ. Code §1798.140(o)(1)(K).

[15] *Id.*. at §1798.140(m).

[16] *Id.* at §1798.110(c).

[17] *Id. at* §1798.140(o)(1).

[18] https://www.gibsondunn.com/accelerating-progress-toward-a-long-awaited-federal-regulatory-framework-for-autonomous-vehicles-in-the-united-states/.

[19] H.R. 3388, 115th Cong. (2017).

[20] U.S. Senate Committee on Commerce, Science and Transportation, Press Release, Oct. 24, 2017, available at https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=BA5E2D29-2BF3-4FC7-A79D-58B9E186412C.

[21] Sean O'Kane, *Mercedes-Benz Self-Driving Taxi Pilot Coming to Silicon Valley in 2019*, The Verge, Jul. 11, 2018, available at https://www.theverge.com/2018/7/11/17555274/mercedes-benz-self-driving-taxi-pilot-silicon-valley-2019.

[22] U.S. Dept. of Transp., Automated Driving Systems 2.0: A Vision for Safety 2.0, Sept. 2017, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

[23] *Id.*, at para 2.

[24] U.S. DEPT. OF TRANSP., Preparing for the Future of Transportation: Automated Vehicles 3.0, Oct. 4, 2018, https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

[25] Sasha Lekach, *Waymo's Self-Driving Taxi Service Could Have Some Major Issues*, Mashable, Aug. 28, 2018, available at https://mashable.com/2018/08/28/waymo-self-driving-taxi-problems/#dWzwp.UAEsqM.

[26] Robert L. Rabin, Uber Self-Driving Cars, Liability, and Regulation, Stanford Law School Blog, Mar. 20, 2018, available at https://law.stanford.edu/2018/03/20/uber-self-driving-cars-liability-regulation/.

[27] David Shephardson, *U.S. Regulators Grappling with Self-Driving Vehicle Security*, Reuters. Jul. 10, 2018, available at https://www.reuters.com/article/us-autos-selfdriving/us-regulators-grappling-with-self-driving-vehicle-security-idUSKBN1K02OD.

[28] Richard Blumenthal, Press Release, *Ten Senators Seek Information from Autonomous Vehicle Manufacturers on Their Use of Forced Arbitration Clauses*, Mar. 23, 2018, available at https://www.blumenthal.senate.gov/newsroom/press/release/ten-senators-seek-information-from-autonomous-vehicle-manufacturers-on-their-use-of-forced-arbitration-clauses.

[29] Kevin Krewell, *How Will Autonomous Cars Respond to Emergency Vehicles*, Forbes, Jul. 31, 2018, available at https://www.forbes.com/sites/tiriasresearch/2018/07/31/how-will-autonomous-cars-respond-to-emergency-vehicles/#3eed571627ef.

[30] Michael J. Coren, *All The Things That Still Baffle Self-Driving Cars, Starting With Seagulls*, Quartz, Sept. 23, 2018, available at https://qz.com/1397504/all-the-things-that-still-baffle-self-driving-cars-starting-with-seagulls/.

[31] ghsa, *Preparing For Automated Vehicles: Traffic Safety Issues For States*, Aug. 2018, available at https://www.ghsa.org/sites/default/files/2018-08/Final_AVs2018.pdf.

[32] *Id*., at 7.

[33] Brookings, *The State of Self-Driving Car Laws Across the U.S.*, May 1, 2018, available at https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/.

[34] Aarian Marshall, *Fully Self-Driving Cars Are Really Truly Coming to California*, Wired, Feb. 26, 2018, available at, https://www.wired.com/story/california-self-driving-car-laws/; State of California, Department of Motor Vehicles, Autonomous Vehicles in California, available at https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/bkgd.

[35] SB 151, available at http://www.capitol.tn.gov/Bills/110/Bill/SB0151.pdf.

[36] SB 2205, available at https://legiscan.com/TX/text/SB2205/2017.

[37] SB 219, available at http://www.legis.ga.gov/Legislation/en-US/display/20172018/SB/219.

[38] Tony Peng & Michael Sarazen, *Global Survey of Autonomous Vehicle Regulations*, Medium, Mar. 15, 2018, available at https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9.

[39] KPMG, *Autonomous Vehicles Readiness Index: Assessing Countries' Openness and Preparedness for Autonomous Vehicles*, 2018, ("The US has a highly innovative but largely disparate environment with little predictability regarding the uniform adoption of national standards for AVs. Therefore the prospect of widespread driverless vehicles is unlikely in the near future. However, federal policy and regulatory guidance could certainly accelerate early adoption . . ."), p. 17, available at https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2018/sector/automotive/autonomous-vehicles-readiness-index.pdf.

[40] Stanley White, *Japan Looks to Launch Autonomous Car System in Tokyo by 2020*, Automotive News, Jun. 4, 2018, available at http://www.autonews.com/article/20180604/MOBILITY/180609906/japan-self-driving-car; National Transport Commission Australia, *Automated vehicles in Australia*, available at https://www.ntc.gov.au/roads/technology/automated-vehicles-in-australia/.

[41] The Automated and Electric Vehicles Act 2018, available at http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted; Lexology, *Muddy Road Ahead Part II: Liability Legislation for Autonomous Vehicles in the United Kingdom*, Sept. 21, 2018, https://www.lexology.com/library/detail.aspx?g=89029292-ad7b-4c89-8ac9-eedec3d9113a; *see further* Anne Perkins, Government to Review Law Before Self-Driving Cars Arrive on UK Roads, The Guardian, Mar. 6, 2018, available at https://www.theguardian.com/technology/2018/mar/06/self-driving-cars-in-uk-riding-on-legal-review.

[42] Michaela Ross, *Code & Conduit Podcast: Rep. Bob Latta Eyes Self-Driving Car Compromise This Year*, Bloomberg Law, Jul. 26, 2018, available at https://www.bna.com/code-conduit-podcast-b73014481132/.

[43] Freight Waves, *House Committee Urges Senate to Advance Self-Driving Vehicle Legislation*, Sept. 10, 2018, available at https://www.freightwaves.com/news/house-committee-urges-senate-to-advance-self-driving-vehicle-legislation; House Energy and Commerce Committee, Press Release, Sept. 5, 2018, available at https://energycommerce.house.gov/news/press-release/media-advisory-walden-ec-leaders-to-call-on-senate-to-pass-self-driving-car-legislation/.

[44] *See supra* n. 24, U.S. DEPT. OF TRANSP., Preparing for the Future of Transportation: Automated Vehicles 3.0, Oct. 4, 2018, iv.

[45] David Shephardson, *Self-driving cars may hit U.S. roads in pilot program, NHTSA says*, Automotive News, Oct. 9, 2018, available at http://www.autonews.com/article/20181009/MOBILITY/181009630/self-driving-cars-may-hit-u.s.-roads-in-pilot-program-nhtsa-says.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, or the authors:

H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Claudia M. Barrett - Washington, D.C. (+1 202-887-3642, cbarrett@gibsondunn.com)
Frances Annika Smithson - Los Angeles (+1 213-229-7914, fsmithson@gibsondunn.com)
Ryan K. Iwahashi - Palo Alto (+1 650-849-5367, riwahashi@gibsondunn.com)

Please also feel free to contact any of the following:

Automotive/Transportation:
Theodore J. Boutrous, Jr. - Los Angeles (+1 213-229-7000, tboutrous@gibsondunn.com)
Christopher Chorba - Los Angeles (+1 213-229-7396, cchorba@gibsondunn.com)
Theane Evangelis - Los Angeles (+1 213-229-7726, tevangelis@gibsondunn.com)

Privacy, Cybersecurity and Consumer Protection:
Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)

Public Policy:
Michael D. Bopp - Washington, D.C. (+1 202-955-8256, mbopp@gibsondunn.com)
Mylan L. Denerstein - New York (+1 212-351-3850, mdenerstein@gibsondunn.com)