

ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS LEGAL UPDATE (1Q19)

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 (“AI”). As noted in our [Artificial Intelligence and Autonomous Systems Legal Update \(4Q18\)](#), we witnessed few notable legislative developments in 2018, but also tentative evidence of growing federal government attention paid to AI technologies, and increasingly tangible steps taken by policy organizations and technology companies to address strategic concerns in light of the lack of a federal AI strategy and regulatory vacuum. Meanwhile, and as we will address in a forthcoming client alert, the past year has seen a significant uptick in global AI policymaking, as numerous world economies made budgetary and policy commitments and sought to stake out a position in the absence of a clear U.S. strategy. Notwithstanding these rapid global developments, its continued leadership position in development of AI technologies —albeit one that is increasingly coming under threat—means the United States still retains a unique opportunity to shape AI’s global impact. In this update, we cover some of the recent developments that sketch out the beginnings of a U.S. federal AI strategy, and provide an overview of key current regulatory and policy issues.

Table of Contents

- I. U.S. National Policy on AI Begins to Take Shape
- II. Recent Bias Concerns for AI
- III. Autonomous Vehicles
- IV. Ethics and Data Privacy

I. U.S. National Policy on AI Begins to Take Shape

Under increasing pressure from the U.S. technology industry and policy organizations to present a substantive federal AI strategy on AI, in the past several months the Trump administration and congressional lawmakers have taken public actions to prioritize AI and automated systems. Most notably, these pronouncements include President Trump’s “Maintaining American Leadership in

Artificial Intelligence” Executive Order^[1] and creation of AI.gov.^[2] While it may be too early to assess the impact of these executive branch efforts, other executive agencies appear to have responded to the call for action. For example, in February, the Department of Defense (“DOD”) detailed its AI strategy and on March 6 to 7, the Pentagon’s research arm, the Defense Advanced Research Projects Agency (“DARPA”), hosted an Artificial Intelligence Colloquium to publicly discuss AI.^[3] The clear interest asserted by the Trump administration and growing traction within executive agencies should provide encouragement to stakeholders that the federal government is willing to prioritize AI, although the extent to which it will provide government expenditures to support its vision remains unclear.

A. President Trump’s Executive Order

On February 11, 2019, President Trump signed an executive order (“EO”), titled “Maintaining American Leadership in Artificial Intelligence.”^[4] The purpose of the EO was to spur the development and regulation of artificial intelligence, machine learning and deep learning and fortify the United States’ global position by directing federal agencies to prioritize investments in AI,^[5] interpreted by many observers to be a response to China’s recent efforts to claim a leadership position in AI research and development.^[6] Observers particularly noted that many other countries preceded the United States in rolling out national AI strategy.^[7] In an apparent response to these concerns, the Trump administration warned in rolling out the campaign that “as the pace of AI innovation increase around the world, we cannot sit idly by and presume that our leadership is guaranteed.”^[8]

To secure U.S. leadership, the EO prioritizes five key areas:

(1) **Investing in AI Research and Development (“R&D”)**: encouraging federal agencies to prioritize AI investments in their “R&D missions” to encourage “sustained investment in AI R&D in collaboration with industry, academia, international partners and allies, and other non-federal entities to generate technological breakthroughs in AI and related technologies and to rapidly transition those breakthroughs into capabilities that contribute to our economic and national security.”^[9]

(2) **Unleashing AI Resources**: making federal data and models more accessible to the AI research community by “improv[ing] data and model inventory documentation to enable discovery and usability” and “prioritiz[ing] improvements to access and quality of AI data and models based on the AI research community’s user feedback.”^[10]

(3) **Setting AI Governance Standards**: aiming to foster public trust in AI by using federal agencies to develop and maintain approaches for safe and trustworthy creation and adoption of new AI technologies (for example, the EO calls on the National Institute of Standards and Technology (“NIST”) to lead the development of appropriate technical standards).^[11]

(4) **Building the AI Workforce**: asking federal agencies to prioritize fellowship and training programs to prepare for changes relating to AI technologies and promoting Science, Technology, Engineering and Mathematics education.^[12]

(5) **International Engagement and Protecting the United States’ AI Advantage:** calling on agencies to collaborate with other nations but also to protect the nation’s economic security interest against competitors and adversaries.[13]

AI developers will need to pay close attention to the executive branch’s response to standards setting. The primary concern for standards sounds in safety, and the AI Initiative echoes this with a high-level directive to regulatory agencies to establish guidance for AI development and use across technologies and industrial sectors, and highlights the need for “appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies”[14] and “foster public trust and confidence in AI technologies.”[15] However, the AI Initiative is otherwise vague about how the program plans to ensure that responsible development and use of AI remain central throughout the process, and the extent to which AI policy researchers and stakeholders (such as academic institutions and nonprofits) will be invited to participate. The EO announces that the NIST will take the lead in standards setting. The Director of NIST, shall “issue a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies” with participation from relevant agencies as the Secretary of Commerce shall determine.[16] The plan is intended to include “Federal priority needs for standardization of AI systems development and deployment,” the identification of “standards development entities in which Federal agencies should seek membership with the goal of establishing or supporting United States technical leadership roles,” and “opportunities for and challenges to United States leadership in standardization related to AI technologies.”[17]

Observers have criticized the EO for its lack of actual funding commitments, precatory language, and failure to address immigration issues for AI firms looking to retain foreign students and hire AI specialists.[18] For example, unlike the Chinese government’s commitment of \$150 billion for AI prioritization, the EO adds no specific expenditures, merely encouraging certain offices to “budget” for AI research and development.[19] To begin to close this gap, on April 11, 2019, Congressmen Dan Lipinski (IL-3) and Tom Reed (NY-23) introduced the Growing Artificial Intelligence Through Research (GrAITR) Act to establish a coordinated federal initiative aimed at accelerating AI research and development for U.S. economic and national security. The GrAITR Act (H.R. 2202) would create a strategic plan to invest \$1.6 billion over 10 years in research, development, and application of AI across the private sector, academia and government agencies, including NIST, the National Science Foundation, and the Department of Energy (DOE)—aiming to help the United States catch up to other countries, including the UK, who are “already cultivating workforces to create and use AI-enabled devices.” The bill has been referred to the House Committee on Science, Space, and Technology. [19a]

In April 2019, Dr. Lynne Parker, assistant director for artificial intelligence at the White House Office of Science and Technology Policy, noted that regulatory authority will be left to agencies to adjust to their sectors, but with high-level guidance from the Office of Management and Budget (“OMB”) on creating a balanced regulatory environment, and agency-level implementation plans. Dr. Parker said that a draft version of OMB’s guidance likely would come out in early summer.[20]

For more details, please see our recent update [President Trump Issues Executive Order on “Maintaining American Leadership in Artificial Intelligence.”](#)

B. AI.gov Launch

On March 19, 2019, the White House launched ai.gov as a platform to share AI initiatives from the Trump administration and federal agencies.[21] These initiatives track along the key points of the AI EO, and ai.gov is intended to function as an ongoing press release. Presently, the website includes five key domains for AI development: the Executive order on AI, AI for American Innovation, AI for American Industry, AI for the American Worker, and AI with American Values.[22]

These initiatives highlight a number of federal government efforts under the Trump administration (and some launched during the Obama administration). Highlights include the White House's charting of a Select Committee on AI under the National Science and Technology Council, the Department of Energy's efforts to develop supercomputers, the Department of Transportation's efforts to integrate automated driving systems, and the Food and Drug Administration's efforts to assess AI implementation in medical research.[23]

C. U.S. Senators Introduce “Algorithmic Accountability Act” to Address Bias

On April 10, 2019, a number of Senate Democrats introduced the Algorithmic Accountability Act, which “requires companies to study and fix flawed computer algorithms that result in inaccurate, unfair, biased or discriminatory decisions impacting Americans.”[24] The bill stands to be the United States Congress's first serious foray into the regulation of AI and the first legislative attempt in the United States to impose regulation on AI systems in general, as opposed to regulating a specific activity, such as autonomous vehicles. While observers have noted congressional reticence to regulate AI in past years, the bill hints at a dramatic shift in Washington's stance amid growing public awareness for AI's potential to create bias or harm certain groups.[25]

The bill casts a wide net, such that many technology companies would find common practices to fall within the purview of the Act. The Act would not only regulate AI systems but also any “automated decision system,” which is broadly defined as any “computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers.”[26] This could conceivably include crude decision tree algorithms. For processes within the definition, companies would be required to audit for bias and discrimination and take corrective action to resolve these issues, when identified. The bill would allow regulators to take a closer look at any “[h]igh-risk automated decision system”—those that involve “privacy or security of personal information of consumers[,]” “sensitive aspects of [consumers'] lives, such as their work performance, economic situation, health, personal preferences, interests, behavior, location, or movements[,]” “a significant number of consumers regarding race [and several other sensitive topics],” or “systematically monitors a large, publicly accessible physical place[.]”[27] For these “high-risk” topics, regulators would be permitted to conduct an “impact assessment” and examine a host of proprietary aspects relating to the system.[28] Additional regulations will be needed to give these key terms meaning but, for now, the bill is a harbinger for AI regulation that identifies key areas of concern for lawmakers.

The bill has some teeth—it would give the Federal Trade Commission the authority to enforce and regulate these audit procedures and requirements—but does not provide for a private right of action or enforcement by state attorneys general.[29] While the political viability of the bill is questionable, Senate Republicans have also recently renewed their scrutiny of technology companies for alleged political bias.[30] At a minimum, companies operating in this space should certainly anticipate further congressional action on this subject in the near future, and proactively consider how their own “high-risk” systems may raise concerns related to bias. In addition, companies may also wish to consider whether and how they ensure that their voice is heard and considered in future legislative efforts.

D. House Subcommittee Hears Testimony About How AI Can Combat Financial Crime

The EO’s promised availability of governmental data may also prove beneficial for those in certain AI industries that are looking to expand their datasets beyond private data.[31] This may be particularly relevant for agencies that have already expressed interest in data collection to ensure AI safety (*e.g.*, in the context of the regulation of autonomous vehicles by the National Highway Traffic Safety Administration (“NHTSA”)). Some AI businesses are now making their request for data access known. On March 13, 2019, the National Security, International Development and Monetary Policy Subcommittee heard testimony from Gary Shiffman, founder and CEO of an AI security firm, who urged the government to implement AI to combat financial crimes, money laundering, trafficking and terrorism, noting that in order to advance this type of AI technology, the government forms an important, and perhaps necessary, part in making the AI systems by providing training data sets.[32] In due course, companies whose products require access to public datasets may well be able to take advantage of emerging partnerships between the federal government and private sector.

E. DOD and DARPA Detail AI Efforts

On February 12, 2019, the DOD unveiled its AI strategy, which builds on the recent EO.[33] The DOD’s chief information officer explained that “[t]he [executive order] is paramount for our country to remain a leader in AI, and it will not only increase the prosperity of our nation, but also enhance our national security. . . .”[34] To that end, the DOD’s plan announced that it will adopt AI to maintain its strategic position.[35] To operationalize that goal, the DOD will rely on the Joint Artificial Intelligence Center and highlighted a key role for academic and industry partners.[36]

In early 2019, DARPA launched a major project called Guaranteeing AI Robustness against Deception (“GARD”), aimed at studying adversarial machine learning. Adversarial machine learning, an area of growing interest for government machine-learning researchers, involves experimentally feeding input into an algorithm to reveal the information on which it has been trained, or distorting input in a way that causes the system to misbehave. With a growing number of military systems—including sensing and weapons systems—harnessing machine learning, there is huge potential for these techniques to be used both defensively and offensively. Hava Siegelmann, Director of the GARD program, told MIT Technology Review recently that the goal of this project was to develop AI models that are robust in the face of a wide range of adversarial attacks, rather than simply able to defend against specific ones.[37]

II. Recent Bias Concerns for AI

As noted above, the recently introduced Algorithmic Accountability Act would require that companies audit any automated decision-making for bias and discrimination. A number of similar developments at national, state and international levels evidence the growing concern with this subject matter, and companies who currently use or are considering using AI to automate decision-making processes should track these developments closely. We are closely monitoring the trends and developments in these areas and stand ready to assist company efforts to anticipate and navigate likely future requirements and concerns to avoid improper bias and discrimination.

A. The AI Now Institute at New York University Publishes New Report, “Discriminating Systems: Gender, Race, and Power in AI”

The AI Now Institute, which examines the social implications of artificial intelligence, recently published a report that examines the scope and scale of the gender and racial diversity crisis in the AI sector and discusses how the use of AI systems for the classification, detection, and prediction of race and gender is in urgent need of re-evaluation. The report includes recommendations for improving workplace diversity (such as publishing harassment and discrimination transparency reports, changing hiring practices to maximize diversity, and being transparent around hiring, compensation, and promotion practices) and recommendations for addressing bias and discrimination in AI systems (such as implementing rigorous testing across the lifecycle of AI systems).[38]

B. Several Government Agencies Seek to Root Out Bias in Artificial Intelligence Systems

In companion bills SB-5527 and HB-1655, introduced on January 23, 2019, Washington State lawmakers drafted a comprehensive piece of legislation aimed at governing the use of automated decision systems by state agencies, including the use of automated decision-making in the triggering of automated weapon systems.[39] In addition to addressing the fact that eliminating algorithmic-based bias requires consideration of fairness, accountability, and transparency, the bills also include a private right of action.[40] According to the bills’ sponsors, automated decision systems are rapidly being adopted to make or assist in core decisions in a variety of government and business functions, including criminal justice, health care, education, employment, public benefits, insurance, and commerce,[41] and are often unregulated and deployed without public knowledge.[42] Under the new law, in using an automated decision system, an agency would be prohibited from discriminating against an individual, or treating an individual less favorably than another on the basis of one or more of a list of factors such as race, national origin, sex, or age.[43] Currently, the bills remain in Committee.[44]

In the UK, the world’s first Centre for Data Ethics and Innovation will partner with the UK Cabinet Office’s Race Disparity Unit to explore potential for bias in algorithms in crime and justice, financial services, recruitment and local government.[45] The UK government explained that this investigation was necessary because of the risk that human bias will be reflected in the recommendations used in the algorithms.[46]

C. Artificial Intelligence Ethics in Policing

Police departments often use predictive algorithms for various other functions, such as to help identify suspects. While such technologies can be useful, there is increasing awareness building with regard to the risk of biases and inaccuracies.[47]

In a paper released on February 13, researchers at the AI Now Institute, a research center that studies the social impact of artificial intelligence, found that police across the United States may be training crime-predicting AIs on falsified “dirty” data,[48] calling into question the validity of predictive policing systems and other criminal risk-assessment tools that use training sets consisting of historical data.[49]

In some cases, police departments had a culture of purposely manipulating or falsifying data under intense political pressure to bring down official crime rates. In New York, for example, in order to artificially deflate crime statistics, precinct commanders regularly asked victims at crime scenes not to file complaints. In predictive policing systems that rely on machine learning to forecast crime, those corrupted data points become legitimate predictors, creating “a type of tech-washing where people who use these systems assume that they are somehow more neutral or objective, but in actual fact they have ingrained a form of unconstitutionality or illegality.”[50]

III. Autonomous Vehicles

The autonomous vehicle (“AV”) industry continues to expand at a rapid pace, with incremental developments towards full autonomy. At this juncture, most of the major automotive manufacturers are actively exploring AV programs and conducting extensive on-road testing. As lawmakers across jurisdictions grapple with emerging risks and the challenge of building legal frameworks and rules within existing, disparate regulatory ecosystems, common challenges are beginning to emerge that have the potential to shape not only the global automotive industry over the coming years, but also broader strategies and policies relating to infrastructure, data management and safety.

A. Legislative Activity at Federal Level

As we reported in our *Artificial Intelligence and Autonomous Systems Legal Update* (3Q18), there was a flurry of legislative activity in Congress in 2017 and early 2018 towards a national regulatory framework. The U.S. House of Representatives passed the Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution (SELF DRIVE) Act[51] by voice vote in September 2017, but its companion bill (the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act),[52] stalled in the Senate as a result of holds from Democratic senators who expressed concerns that the proposed legislation remains immature and underdeveloped in that it “indefinitely” preempts state and local safety regulations even in the absence of federal standards.[53] So far, there have been no attempts to reintroduce the bill in the new congressional session, and even if efforts to reintroduce it are ultimately successful, the measure may not be enough to assuage safety concerns as long as it lacks an enforceable federal safety framework.

Therefore, AVs continue to operate under a complex patchwork of state and local rules, with federal oversight limited to the U.S. Department of Transportation’s (“DoT”) informal guidance. As we

reported in our *Artificial Intelligence and Autonomous Systems Legal Update (4Q18)*, the DoT’s NHTSA released its road map on the design, testing and deployment of driverless vehicles: “Preparing for the Future of Transportation: Automated Vehicles 3.0” (commonly referred to as “AV 3.0”) on October 3, 2018.[54] However, while AV 3.0 reinforces that federal officials are eager to take the wheel on safety standards and that any state laws on automated vehicle design and performance will be preempted, the thread running throughout is the commitment to voluntary, consensus-based technical standards and the removal of unnecessary barriers to the innovation of AV technologies.

B. Legislative Activity at State and Local Levels

Recognizing that AVs and vehicles with semi-autonomous components are already being tested and deployed on roads amid legislative gridlock at federal level, thirty states and the District of Columbia have enacted autonomous vehicle legislation, while governors in at least 11 states have issued executive orders on self-driving vehicles.[55] In 2019 alone, 75 new bills in 20 states have ‘pending’ status.[56] Currently, ten states authorize testing, while 14 states and the District of Columbia authorize full deployment. 16 states now allow testing or deployment without a human operator in the vehicle, although some limit it to certain defined conditions.[57] Increasingly, there are concerns that states may be racing to cement their positions as leaders in AV testing in the absence of a federal regulatory framework by introducing increasingly permissive bills that allow testing without human safety drivers.[58]

Some states are explicitly tying bills to federal guidelines in anticipation of congressional action. On April 2, 2019, D.C. lawmakers proposed the Autonomous Vehicles Testing Program Amendment Act of 2019, which would set up a review and permitting process for autonomous vehicle testing within the District Department of Transportation. Companies seeking to test self-driving cars in the city would have to provide an array of information to officials, including— for each vehicle it plans to test—safety operators in the test vehicles, testing locations, insurance, and safety strategies.[59] Crucially, it would require testing companies to certify that their vehicles comply with federal safety policies; share with officials data on trips and any crash or cybersecurity incidents; and train operators on safety.[60]

Moreover, cities—who largely control the test sites—are creating an additional layer of rules for AVs, ranging from informal agreements to structured contracts between cities and companies, as well as zoning laws.[61] Given the fast pace of developments and tangle of applicable rules, it is essential that companies operating in this space stay abreast of legal developments in states as well as cities in which they are developing or testing autonomous vehicles, while understanding that any new federal regulations may ultimately preempt states’ authorities to determine, for example, safety policies or how they handle their passengers’ data. We will continue to carefully monitor significant developments in this space.

C. Increasing Focus on Connectivity and Infrastructure in AV Development

AVs operate by several interconnected technologies, including sensors and computer vision (e.g. radars, cameras and lasers), deep learning and other machine intelligence technologies, robotics and navigation (e.g. GPS). As lawmakers debate how to integrate AVs into existing infrastructure, a key emerging

regulatory challenge is “connectivity.” While AV technology resides largely onboard the vehicle itself, and sensor systems are rapidly evolving to meet the demands of AV operations, fully autonomous vehicles nonetheless require sufficient network infrastructure to communicate efficiently with their surroundings (i.e. to communicate with infrastructure, such as traffic lights and signage, and vehicle-to-vehicle, collectively known as Vehicle-to-Everything communication, or “V2X”).^[62]

At present, there are two competing technical standards for V2X on the European market: ITS-G5 Wi-Fi standard and the alternative “C-V2X” standard (“Cellular Vehicle-to-Everything”). C-V2X is designed to work with 5G wireless technology but is incompatible with Wi-Fi. There is presently neither regulatory nor industry consensus on this topic. A group of automakers, the 5G Automotive Association, now counts more than 100 members who argue that C-V2X is preferable to Wi-Fi in terms of security, reliability, range and reaction time.^[63] However, in April 2019, the European Commission proposed a legal act to regulate so-called “Cooperative-Intelligent Transport Systems (C-ITS),” backing the ITS-G5 Wi-Fi standard.^[64]

By contrast, in the United States, the AV 3.0 guidelines acknowledged that private sector companies were already researching and testing C-V2X technology alongside the Dedicated Short-Range Communication (“DSRC”)-based deployments, but also cautioned that while V2X is an important complementary technology that is expected to enhance the benefits of automation at all levels, “it should not be and realistically cannot be a precondition to the deployment of automated vehicles” and that DoT “does not promote any particular technology over another.”^[65] This approach appears to be in line with the DoT’s overarching desire to remain “technologically neutral” to avoid interfering with innovation. Nonetheless, in December 2018, the DoT announced that it was seeking public comment on V2X communications,^[66] noting that “there have been developments in core aspects of the communication technologies needed for V2X, which have raised questions about how the Department can best ensure that the safety and mobility benefits of connected vehicles are achieved without interfering with the rapid technological innovations occurring in both the automotive and telecommunications industries,” including in both C-V2X and “5G” communications, which “may, or may not, offer both advantages and disadvantages over DSRC.”^[67]

Meanwhile, AVs built in China—which has set a goal of 10% of vehicles reaching Level 4/5 autonomy by 2030—will support the C-V2X standard, and will likely be developed in an ecosystem of infrastructure, technical standards and regulatory requirements distinct from those of their European counterparts.^[68] In addition to setting a national DSRC standard, China also plans to cover 90% of the country with C-V2X sensors by 2020.^[69] In 2017, the Chinese government called for more than 100 domestic standards for AVs and other internet-connected vehicles. Instead of GPS, AVs will support China’s BeiDou GNSS standard — which requires different receiver chips to communicate with Chinese satellites. Major Chinese cities also enforce license plate jurisdiction and have roads and lanes dedicated to specific vehicle types, allowing for more effective geo-fencing of AV testing and operating areas. AV companies will have to engage with forthcoming standards and development plans from China’s Ministry of Industry of Information Technology, its AV-coordinating commission (the “Internet of Vehicles Development Commission”), and quasi-private industry groups.^[70]

Given the lack of international (or even national) consensus and the potential burden of developing and installing different systems in vehicles for domestic markets and for export, companies operating in the AV space should remain alert to developments in this rapidly evolving landscape of technical standards and infrastructure.

IV. Ethics and Data Privacy

The rapidly expanding uses for artificial intelligence, both personal and professional, raise a number of issues for governments worldwide and also for companies attempting to navigate an evolving ethics landscape, including threats to data privacy as well as calls for transparency and accountability.

A. Government Regulation of Artificial Intelligence

The United States continues to be a key player and dominant force in the development of artificial intelligence, and the U.S. government continues to identify AI as a key concern when it comes to cybersecurity and data privacy. For example, the Office of the Director of National Intelligence, recently highlighted, in its 2019 “National Intelligence Strategy” report, that U.S. adversaries benefit from that AI-created military and intelligence capabilities, and emphasized that such capabilities pose significant threats to U.S. interests.^[71] But despite this key role in the development of emerging technologies, and the threats faced by the United States, there has been little by way of public guidance or regulation of AI, at least on the federal level.^[72]

In contrast, the European Union (“EU”) has recently issued guidance on ethical considerations in the use of AI. In connection with the implementation of its General Data Privacy Rules (“GDPR”) in 2018, the EU recently released a report from its “High-Level Expert Group on Artificial Intelligence”: the EU “Ethics Guidelines for Trustworthy AI” (“Guidelines”).^[73] The Guidelines lay out seven ethical principles “that must be respected in the development, deployment, and use of AI systems”:

- (1) **Human Agency and Oversight:** AI systems should enable equitable societies by supporting human agency and fundamental rights, and not decrease, limit or misguide human autonomy.
- (2) **Robustness and Safety:** Trustworthy AI requires algorithms to be secure, reliable and robust enough to deal with errors or inconsistencies during all life cycle phases of AI systems.
- (3) **Privacy and Data Governance:** Citizens should have full control over their own data, while data concerning them will not be used to harm or discriminate against them.
- (4) **Transparency:** The traceability of AI systems should be ensured.
- (5) **Diversity, Non-Discrimination and Fairness:** AI systems should consider the whole range of human abilities, skills and requirements, and ensure accessibility.
- (6) **Societal and Environmental Well-Being:** AI systems should be used to enhance positive social change and enhance sustainability and ecological responsibility.

(7) **Accountability:** Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.

In addition to laying out these principles, the Guidelines highlight the importance of implementing a “large-scale pilot with partners” and of “building international consensus for human-centric AI.”^[74] Specifically, the Commission will launch a pilot phase of guideline implementation in Summer 2019, working with “like-minded partners such as Japan, Canada or Singapore.”^[75] The EU also intends to “continue to play an active role in international discussions and initiatives including the G7 and G20.”^[76]

While the Guidelines do not appear to create any binding regulation on stakeholders in the EU, their further development and evolution will likely shape the final version of future regulation throughout the EU. Therefore, the Summer 2019 pilot program, as well as any further international work between the EU and other partners, merits continued attention.

B. DARPA Prioritizes Ethics in AI Development

DARPA hosted an Artificial Intelligence Colloquium from March 6-7, 2019 in Alexandria, Virginia, to increase awareness of DARPA’s expansive AI R&D efforts.^[77] During the weeks after the colloquium, several news sources reported on DARPA’s AI research and technology. In an interview discussing DARPA’s AI-infused drones that would be used to map combatants and civilians in the field, the agency discussed how ethics is informing its development and implementation of AI systems.^[78] DARPA highlighted that they met with ethicists before advancing technical development of the technology.^[79]

C. UN Urges Ban on Autonomous Weapons that Kill

The United Nations Secretary-General António Guterres has urged restriction on the development of lethal autonomous weapons systems, or LAWS,^[80] arguing that machines with the power and discretion to take lives without human involvement are politically unacceptable, morally repugnant and should be prohibited by international law.^[81] Subsequently, Japan pledged that it will not develop fully automated weapons systems.^[82] A group of member states—including the UK, United States, Russia, Israel and Australia—are reportedly opposed to a preemptive ban in the absence of any international agreement on the characteristics of autonomous weapons.^[83]

[1] Donald J. Trump, *Executive Order on Maintaining American Leadership in Artificial Intelligence*, The White House (Feb. 11, 2019), Exec. Order No. 13859, 3 C.F.R. 3967, available at <https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/>

[2] Jon Fingas, *White House Launches Site to Highlight AI Initiatives*, Endgadget (Mar. 20, 2019), available at <https://www.engadget.com/2019/03/20/white-house-ai-gov-website/>.

GIBSON DUNN

[3] Paulina Glass, *Here's the Key Innovation in DARPA AI Project: Ethics From the Start*, Defense One (Mar. 15, 2019), available at <https://www.defenseone.com/technology/2019/03/heres-key-innovation-darpas-ai-project-ethics-start/155589/>.

[4] *Supra*, n.1.

[5] The White House, *Accelerating America's Leadership in Artificial Intelligence*, Office of Science and Technology Policy (Feb. 11, 2019), available at <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-accelerating-americas-leadership-in-artificial-intelligence/>.

[6] *See, e.g.*, Jamie Condliffe, *In 2017, China is Doubling Down on AI*, MIT Technology Review (Jan. 17, 2017), available at <https://www.technologyreview.com/s/603378/in-2017-china-is-doubling-down-on-ai/>; Cade Metz, *As China Marches Forward on A.I., the White House Is Silent*, N.Y. Times (Feb. 12, 2018), available at <https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html?module=inline>.

[7] Jessica Baron, *Will Trump's New Artificial Intelligence Initiative Make The U.S. The World Leader In AI?*, Forbes (Feb. 11, 2019), available at <https://www.forbes.com/sites/jessicabaron/2019/02/11/will-trumps-new-artificial-intelligence-initiative-make-the-u-s-the-world-leader-in-ai/#70d3ea99a017> (noting that, after Canada in March 2017, the United States will be the 19th country to announce a formal strategy for the future of AI); *see also*, as noted in our recent Artificial Intelligence and Autonomous Systems Legal Update (4Q18), the German government's new AI strategy, published in November 2018, which promises an investment of €3 billion before 2025 with the aim of promoting AI research, protecting data privacy and digitalizing businesses (available at <https://www.bundesregierung.de/breg-en/chancellor/ai-a-brand-for-germany-1551432>).

[8] *Supra*, n.5.

[9] *Supra*, n.1

[10] *Supra*, n.1 at 3969.

[11] *Id.* at 3970.

[12] *Id.* at 3971.

[13] *Id.*

[14] *Id.* at 3967.

[15] *Id.*

[16] *Id.* at 3970.

[17] *Id.*

GIBSON DUNN

[18] See, e.g., James Vincent, *Trump Signs Executive Order to Spur US Investment in Artificial Intelligence*, The Verge (Feb. 11, 2019); Oren Etzioni, *What Trump’s Executive Order on AI Is Missing*, Wired (Feb. 13, 2019), available at <https://www.wired.com/story/what-trumps-executive-order-on-ai-is-missing/>.

[19] Darrell M. West, *Assessing Trump’s Artificial Intelligence Executive Order*, The Brookings Institute (Feb. 12, 2019) available at <https://www.brookings.edu/blog/techtank/2019/02/12/assessing-trumps-artificial-intelligence-executive-order/>.

[19a] H.R. 2022, 116th Cong. (2019). For more details, see <https://www.congress.gov/bill/116th-congress/house-bill/2202> or <https://lipinski.house.gov/press-releases/lipinski-introduces-bipartisan-legislation-to-bolster-us-leadership-in-ai-research/>.

[20] *White House AI Order Emphasizes Use for Citizen Experience*, Meritalk (Apr. 18, 2019), available at <https://www.meritalk.com/articles/white-house-ai-order-emphasizes-use-for-citizen-experience/>.

[21] Khari Johnson, *The White House Launches ai.gov*, VentureBeat (Mar. 19, 2019), available at <https://venturebeat.com/2019/03/19/the-white-house-launches-ai-gov/>.

[22] Donald J. Trump, *Artificial Intelligence for the American People*, the White House (2019), available at <https://www.whitehouse.gov/ai/>.

[23] *Id.*; see further our previous legal updates for more details on some of these initiatives: <https://www.gibsondunn.com/?search=news&s=&practice%5B%5D=36270>.

[24] Cory Booker, *Booker, Wyden, Clarke Introduce Bill Requiring Companies To Target Bias In Corporate Algorithms*, United States Senate (Apr. 10, 2019), available at https://www.booker.senate.gov/?p=press_release&id=903; see also S. Res. ___, 116th Cong. (2019).

[25] See, e.g., Karen Hao, *Congress Wants To Protect You From Biased Algorithms, Deepfakes, And Other Bad AI*, MIT Review (Apr. 15, 2019), available at <https://www.technologyreview.com/s/613310/congress-wants-to-protect-you-from-biased-algorithms-deepfakes-and-other-bad-ai/>; Meredith Whittaker, Et Al., *AI Now Report 2018*, AI Now Institute, 2.2.1 (Dec. 2018), available at https://ainowinstitute.org/AI_Now_2018_Report.pdf; Russell Brandom, *Congress Thinks Google Has a Bias Problem—Does It?*, The Verge (Dec. 12, 2018), available at <https://www.theverge.com/2018/12/12/18136619/google-bias-sundar-pichai-google-hearing>.

[26] *Supra*, n.24.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] Tony Roman, *Senate Republicans Renew Their Claims that Facebook, Google and Twitter Censor Conservatives*, The Washington Post (Apr. 10, 2019), available at https://www.washingtonpost.com/technology/2019/04/10/facebook-google-twitter-under-fire-senate-republicans-censoring-conservatives-online/?utm_term=.69aa442c36a5.

[31] *Supra*, n.1 at 3969 (stating that “[h]eads of all agencies shall review their Federal data and models to identify opportunities to increase access and use by the greater non-Federal AI research community in a manner that benefits that community, while protecting safety, security, privacy, and confidentiality. Specifically, agencies shall improve data and model inventory documentation to enable discovery and usability, and shall prioritize improvements to access and quality of AI data and models based on the AI research community’s user feedback.”).

[32] Amanda Ziadeh, *Giant Oak’s Gary Shiffman Testifies About How AI Can Combat Financial Crime*, WashingtonExec (Mar. 18, 2019), available at <https://washingtonexec.com/2019/03/giant-oaks-gary-shiffman-testifies-about-how-ai-can-combat-financial-crime/>.

[33] Terri Moon Cronk, *DOD Unveils Its Artificial Intelligence Strategy*, The Department of Defense (Feb. 12, 2019) available at <https://dod.defense.gov/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/>.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] Will Knight, *How Malevolent Machine Learning Could Derail AI*, MIT Technology Review (Mar. 25, 2019), available at <https://www.technologyreview.com/s/613170/emtech-digital-dawn-song-adversarial-machine-learning/>

[38] AI Now Institute, *Discriminating Systems: Gender, Race, and Power in AI* (Apr. 2019), available at <https://ainowinstitute.org/discriminatingsystems.pdf>.

[39] See Brian Higgins, *Washington State Seeks to Root Out Bias in Artificial Intelligence Systems, Artificial Intelligence Technology and the Law* (Feb. 6, 2019), available at <http://aitechnologylaw.com/2019/02/washington-state-seeks-to-root-out-bias-in-artificial-intelligence-systems/>.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] DJ Pangburn, *Washington Could Be the First State to Rein in Automated Decision-Making*, Fast Company (February 8, 2019), available at <https://www.fastcompany.com/90302465/washington-introduces-landmark-algorithmic-accountability-laws>; A separate privacy bill stalled in the Washington State House of Representatives, despite having been overwhelmingly approved by the state Senate in March 2019. The bill, which is intended to strengthen consumer rights by regulating how online technology companies collect, use, share and sell consumers' personal information, likely will not be passed in 2019, see Allison Grande, *Washington State Privacy Bill Likely Won't Pass This Year*, Law360 (April 19, 2019), available at <https://www.law360.com/articles/1151755/washington-state-privacy-bill-likely-won-t-pass-this-year>.

[45] Gov.UK, *Investigation launched into potential for bias in algorithmic decision-making in society* (Mar. 20, 2019), available at <https://www.gov.uk/government/news/investigation-launched-into-potential-for-bias-in-algorithmic-decision-making-in-society>.

[46] *Id.*

[47] Karen Hao, *AI Is Sending People To Jail – And Getting It Wrong*, MIT Technology Review (Jan. 21, 2019), available at <https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/>. See also Rod McCullom, *Facial Recognition Technology is Both Biased and Understudied*, UnDark (May 17, 2017), available at <https://undark.org/article/facial-recognition-technology-biased-understudied/>.

[48] See Karen Hao, *Police Across the US Are Training Crime-Predicting AIs on Falsified Data*, MIT Technology Review (Feb. 13, 2019), available at <https://www.technologyreview.com/s/612957/predictive-policing-algorithms-ai-crime-dirty-data/>.

[49] Richardson, Rashida and Schultz, Jason and Crawford, Kate, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice* (Feb. 13, 2019). New York University Law Review Online, Forthcoming, available at SSRN: <https://ssrn.com/abstract=3333423>.

[50] *Supra*, n.48.

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

[52] 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>.

[53] Letter from Democratic Senators to U.S. Senate Committee on Commerce, Science and Transportation (Mar. 14, 2018), available at <https://morningconsult.com/wp-content/uploads/2018/11/2018.03.14-AV-START-Act-letter.pdf>.

GIBSON DUNN

[54] U.S. Dept. of Transp., *Preparing for the Future of Transportation: Automated Vehicles 3.0* (Sept. 2017), available at <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf>; see also <https://www.law360.com/articles/1113438/how-av-3-0-changed-the-autonomous-vehicle-game-in-2018>.

[55] Nat'l Conference of State Legislatures, *Autonomous Vehicles State Bill Tracking Database* (Apr. 9, 2019), available at <http://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx>.

[56] *Id.*

[57] Insurance Institute for Highway Safety, Highway Loss Data Institute, *Automation and Crash Avoidance* (Apr. 2019), available at <https://www.iihs.org/iihs/topics/laws/driving-automation>; for an interactive map showing the status of state laws, see <https://www.iihs.org/iihs/topics/laws/driving-automation/driving-automation-map?topicName=automation-and-crash-avoidance>.

[58] Dan Robitzki, *Florida Law Would Allow Self-Driving Cars With No Safety Drivers*, *Futurism* (Jan. 29, 2019) available at <https://futurism.com/florida-law-self-driving-cars>.

[59] Andrew Glambro, *Self-Driving Cars Are Coming. D.C. Lawmakers Want To Regulate Them*, *Curbed* (Apr. 3, 2019), available at <https://dc.curbed.com/2019/4/3/18294167/autonomous-vehicles-dc-self-driving-cars-regulations>.

[60] *Id.*, see further the Autonomous Vehicles Testing Program Amendment Act of 2019, available at <http://lims.dccouncil.us/Download/42211/B23-0232-Introduction.pdf>.

[61] See, e.g., Rainwater & DuPuis, *Cities Have Taken the Lead in Regulating Driverless Vehicles*, *CityLab* (Oct. 3, 2018), available at <https://www.citylab.com/perspective/2018/10/cities-lead-regulation-driverless-vehicles/573325/>; Jamie Condliffe, *Who Should Let Driverless Cars Off the Leash?*, *NY Times* (Mar. 29, 2019), available at <https://www.nytimes.com/2019/03/29/technology/lyft-autonomous-cars.html>.

[62] *6 Key Connectivity Requirements of Autonomous Driving*, *IEEE Spectrum*, available at <https://spectrum.ieee.org/transportation/advanced-cars/6-key-connectivity-requirements-of-autonomous-driving> (“Industry leaders will need to master connectivity to deliver the V2X (vehicle-to-everything) capabilities fully autonomous driving promises.”).

[63] This position is also supported by the telecommunication lobby GMSA, see Foo Yun Chee, *Telco Lobby Urges EU Lawmakers To Spurn Push For Wifi Car Standard*, *Reuters* (Apr. 9, 2019), available at <https://www.reuters.com/article/us-eu-autos-technology/telco-lobby-urges-eu-lawmakers-to-spurn-push-for-wifi-car-standard-idUSKCN1RL2MH?feedType=RSS&feedName=technologyNews>.

[64] Douglas Busvine, *Explainer: Betting On The Past? Europe Decides On Connected Car Standards*, Reuters (Apr. 18, 2019), available at <https://www.reuters.com/article/us-eu-autos-technology-explainer/explainer-betting-on-the-past-europe-decides-on-connected-car-standards-idUSKCN1RU214>.

[65] *Supra*, n.54 at 13, 16.

[66] U.S. Dept. of Transp., *U.S. Department of Transportation Releases Request for Comment (RFC) on Vehicle-to-Everything (V2X) Communications* (Dec. 18, 2018), available at <https://www.nhtsa.gov/press-releases/us-department-transportation-releases-request-comment-rfc-vehicle-everything-v2x>.

[67] Office of the Federal Register, *Notice of Request for Comments: V2X Communications* (Dec. 12, 2018), available at <https://www.federalregister.gov/documents/2018/12/26/2018-27785/notice-of-request-for-comments-v2x-communications>.

[68] Patrick Lozada, *China's Avs Will Think And Drive Differently*, Axios (Mar. 8, 2019), available at <https://www.axios.com/chinas-av-will-think-and-drive-differently-e0a823b4-df60-4667-b21b-7bbe529e53cd.html>.

[69] *Id.*

[70] Patrick Lozada, *An Obscure Chinese Commission Could Change The Future Of Avs*, Axios (Jan. 18, 2019), available at <https://www.axios.com/an-obscure-chinese-commission-could-change-the-future-of-avs-b7520e56-90cf-4b5a-b523-7c44846e08ec.html>.

[71] Office of the Director of National Security, *National Intelligence Strategy of the United States of America (2019)*, available at https://www.intel.gov/templates/intelgov-template/custom-sections/the-nis-at-a-glance/pdf/National_Intelligence_Strategy_2019.pdf?mod=article_inline.

[72] <https://www.gibsondunn.com/artificial-intelligence-and-autonomous-systems-legal-update-3q18/>.

[73] European Commission, *Ethics Guidelines for Trustworthy AI*, April 8, 2019, available at <https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/04/AIEthicsGuidelinespdf1.pdf>.

[74] *Artificial Intelligence: Commission takes forward its work on ethical guidelines*, Press Release, April 8, 2019, available at http://europa.eu/rapid/press-release_IP-19-1893_en.htm.

[75] *Id.*

[76] *Id.*

GIBSON DUNN

[77] *DARPA Announces 2019 AI Colloquium*, available at <https://www.darpa.mil/news-events/2018-11-16>.

[78] Paulina Glass, *Here's the Key Innovation in DARPA AI Project: Ethics From the Start*, Defense One (Mar. 15, 2019), available at <https://www.defenseone.com/technology/2019/03/heres-key-innovation-darpas-ai-project-ethics-start/155589/>.

[79] *Id.*

[80] *Autonomous Weapons that Kill Must be Banned, Insists UN Chief*, UN News (Mar. 25, 2019), available at <https://news.un.org/en/story/2019/03/1035381>.

[81] *Id.*

[82] *Japan Pledges No AI "Killer Robots," MeriTalk* (Mar. 25, 2019), available at <https://www.meritalk.com/articles/japan-pledges-no-ai-killer-robots/>.

[83] Damien Gayle, *UK, US and Russia among those opposing killer robot ban*, The Guardian (Mar. 29, 2019), available at <https://www.theguardian.com/science/2019/mar/29/uk-us-russia-opposing-killer-robot-ban-un-ai>.



The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Frances A. Waldmann, Tony Bedel, Panayiota Burquier, Martie P. Kutscher, Gatsby Miller and Arjun Rangarajan.

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 any of the following lawyers in the firm's Artificial Intelligence and Automated Systems Group:

*H. Mark Lyon - Chair, Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Frances A. Waldmann - Los Angeles (+1 213-229-7914, fwaldmann@gibsondunn.com)*

© 2019 Gibson, Dunn & Crutcher LLP

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.