GIBSON DUNN

February 11, 2020

2019 ARTIFICIAL INTELLIGENCE AND AUTOMATED SYSTEMS ANNUAL LEGAL REVIEW

To Our Clients and Friends:

In 2019, companies and regulators faced unprecedented challenges as they navigated a rapidly evolving set of issues and policy proposals on the regulation of Artificial Intelligence and Automated Systems ("AI"). Lawmakers grappled with the difficult questions of *how* and *when* to regulate AI and sketched out new legal frameworks, bringing into sharper relief the overarching legal issues that are poised to become the subject of protracted debate over the coming year. The policy debate in 2019 was especially characterized by the gulf between sprawling treatises setting out general ethical principles designed to control and mitigate the risks of AI—including theoretical applications of "general" AI[1]—on the one hand, and calls for targeted restrictions on the specific use of certain "narrow" domain-specific AI products and applications on the other.

In the United States, while federal policy remains "light-touch," lawmakers responded to increasing public concern over the perceived dangers of unfettered technological development by proposing a number of high profile draft bills addressing the role of AI and how it should be governed, the real impact of which is yet to be felt across the private sector. U.S. state and local governments pressed forward with concrete legislative proposals regulating the use of AI. Finally, 2019 saw a growing international consensus that AI technology should be subject to certain technical standards and potentially even certification procedures in the same way other technical systems require certification before deployment.

This inaugural Artificial Intelligence and Automated Systems Annual Legal Review places these, and other, 2019 developments in broader context, focusing on developments within the United States. We also touch, albeit non-exhaustively, on developments within the EU that are of relevance to domestic and international companies alike. The AI policy landscape is vast and fast-evolving—we do not attempt to address every development that occurred in 2019, but examine a number of the most significant developments affecting companies as they navigate the evolving AI landscape.

TABLE OF CONTENTS

I. GLOBAL POLICY DEVELOPMENTS

The past year saw a number of ambitious projects and guidelines from governments and other intergovernmental bodies around the world aiming to identify shared norms and values—described by one such initiative as "holistic definitions of societal prosperity […] versus […] one-dimensional goals of increased productivity or gross domestic product"[2]—in an attempt to reach a global consensus on how to define and then instill an ethical approach into AI development and governance.[3] While these recommendations are non-binding and advisory in nature, their potential impact on national policy-making and, ultimately, concrete regulations, should not be underestimated. We offer a brief overview of several of these policy initiatives in order to place legislative, regulatory and policy approaches proposed and enacted by governments and other domestic regulatory bodies in a broader global context.

A. OECD Recommendations on AI

On May 21, 2019, the 36 member countries of the Organization for Economic Co-operation and Development ("OECD"), along with Argentina, Brazil, Colombia, Costa Rica, Peru and Romania, adopted a set of recommendations on AI referred to as "Principles of Artificial Intelligence" ("Principles").[4] The Principles were drafted by a group of experts comprising experts from different OECD members, disciplines and sectors.[5] Intended to represent the first intergovernmental standard

for AI policies, they promote five strategies for developing national policy and international cooperation, treading the line between promoting economic improvement and innovation and fostering fundamental values and trust in the development of AI: inclusive growth, sustainable development and well-being; human-centered values and fairness; transparency and explainability; robustness, security and safety; and accountability. The Principles are broadly stated and not legally binding, but instead seek to encourage member countries to incorporate these values or ethics in the development of AI.[6]

B. Global Partnership on AI

In May 2019, Canada and France announced plans for a new international body ("Global Partnership on AI") for the G7 countries to study and steer the effects of artificial intelligence on the world's people and economies by creating best practices, modeled on the UN's Intergovernmental Panel on Climate Change.[7] Although the principles espoused by the Global Partnership would not be legally binding on other governments or private companies, the White House has raised concerns that the approach is too restrictive and duplicates work already being done by the OECD, and has so far declined to participate.[8]

C. Global Initiative on Ethics of Autonomous and Intelligent Systems

In 2019, the Institute of Electrical and Electronics Engineers ("IEEE") launched the "Global Initiative on Ethics of Autonomous and Intelligent Systems" in order to "establish societal and policy guidelines in order for such systems to remain human-centric, serving humanity's values and ethical principles."[9] In an extensive report addressing ethical considerations in the design of AI systems, IEEE applied classical ethics and human rights methodologies to considerations of algorithmic design and articulated eight high-level ethical principles that apply to all types of AI products, regardless of whether they are physical robots or software systems, and that "define imperatives for the design, development, deployment, adoption, and decommissioning of [AI]."[10] The eight principles are: human rights, human well-being, data agency and control, effectiveness and fitness for purpose, transparency, accountability, awareness of misuse, and operational competence.[11]

D. UN Considers Ban on Lethal Autonomous Weapons

In March 2019, the United Nations ("UN") Secretary-General António Guterres urged restriction on the development of lethal autonomous weapons systems ("LAWs"), 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.[12] Subsequently, Japan pledged that it will not develop fully automated weapons systems.[13] 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, stalling any progress towards a common approach for the time being.[14]

II. U.S. NATIONAL POLICY & KEY LEGISLATIVE EFFORTS

A. U.S. National Policy on AI Takes Shape

By early 2019, despite its position at the forefront of commercial AI innovation, the United States still lacked an overall federal AI strategy and policy.[15] Under increasing pressure from the U.S. technology industry and policy organizations to present a substantive federal AI strategy on AI, over the past 12 months the Trump administration took public actions to prioritize AI and automated systems. Most notably, these pronouncements include President Trump's "Maintaining American Leadership in Artificial Intelligence" Executive Order[16] and the subsequently issued guidance to federal regulatory agencies.[17] U.S. federal, state and local government agencies also began to show a willingness to take concrete positions on regulation, resulting in a variety of policy approaches – many of which eschew informal guidance and voluntary standards and favor outright technology bans. For the most part, the trend in favor of more individual and nuanced assessments of how best to regulate AI systems specific to their end uses by regulators in the United States has been welcome. Although there is an inherent risk that reactionary legislative responses will result in a disharmonious, fragmented national regulatory framework, such developments will yield important insights into what it means to govern and regulate AI over the coming year.

1. Executive Order "Maintaining American Leadership in Artificial Intelligence"

On February 11, 2019, President Trump signed an executive order ("EO") titled "Maintaining American Leadership in Artificial Intelligence."[18] 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,[19] interpreted by many observers to be a response to China's efforts to claim a leadership position in AI research and development.[20]

The EO, which was titled 'Maintaining American Leadership in Artificial Intelligence,' outlined five key areas: research and development,[21] 'unleashing' AI resources,[22] establishing AI governance standards, building an AI workforce,[23] and international collaboration and protection.[24] The AI Initiative is coordinated through the National Science and Technology Council Select Committee on Artificial Intelligence ("NSTC Select Committee").

While the EO favors broad principles in line with the administration's "light-touch" approach to private sector regulation, AI developers will need to pay close attention to the executive branch's response to standards setting. 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).[25]

In response, in July 2019 NIST sought public comment on a draft plan for federal government engagement in advancing AI standards for U.S. economic and national security needs ("U.S. Leadership in AI: Plan for Federal Engagement in Developing Technical Standards and Related Tools").[26] The plan recommends four actions: bolster AI standards-related knowledge, leadership and coordination

among federal agencies; promote focused research on the "trustworthiness" of AI; support and expand public-private partnerships; and engage with international parties.

The full impact of the AI Initiative is not yet known: while it sets some specific deadlines for formalizing plans by agencies under the direction of the Select Committee, the EO is not self-executing and is generally thin on details. Therefore, the long-term impact will be in the actions recommended and taken as a result of those consultations and reports, not the EO itself.[27] Moreover, although the AI Initiative is designed to dedicate resources and funnel investments into AI research, the EO does not set aside specific financial resources or provide details on how available resources will be structured.

In March 2019, the White House launched ai.gov as a platform to share AI initiatives from the Trump administration and federal agencies.[28] These initiatives track along the key points of the AI EO, and ai.gov is intended to function as an ongoing press release, highlighting a number of federal government efforts under the Trump administration (and some launched during the Obama administration): the White House's charting of the NSTC Select Committee on AI, 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.[29]

2. The GrAITR Act (H.R. 2202)

The Growing Artificial Intelligence Through Research (GrAITR) Act was introduced in April 2019 to establish a coordinated federal initiative aimed at accelerating AI research and development for US economic and national security and closing the existing funding gap.[30] The Act 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, and the National Science Foundation and the Department of Energy – aimed at helping the United States catch up to other countries, including the United Kingdom, 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.[31]

3. Artificial Intelligence Initiative Act (S. 1558)

In May 2019, U.S. Senators Rob Portman (R-OH), Martin Heinrich (D-NM), and Brian Schatz (D-HI) proposed a companion bill to GrAITR, the Artificial Intelligence Initiative Act, which would attempt to create a national, overarching strategy 'tailored to the US political economy', for developing AI with a $2.2 billion federal investment over the next five years.[32] The Act would task branches of the federal government to use AI where possible in operation of its systems. Specifically, it includes the establishment of a national office to coordinate AI efforts across the federal system (National AI Coordination Office), requests that NIST establish ethical standards and identify metrics used to establish standards for evaluating AI algorithms and their effectiveness, as well as the quality of training data sets, and proposes that the National Science Foundation set educational goals for AI and STEM learning.[33] Moreover, the bill requires the Department of Energy to create an AI research program, building state-of-the-art computing facilities that will be made available to private sector users on a cost-recovery basis.[34] The draft legislation complements the formation of the bipartisan Senate AI Caucus in March

2019 to address transformative technology with implications spanning a number of fields including transportation, healthcare, agriculture, manufacturing and national security.

4. AI in Government Act (H.R. 2575/S. 3502)

House Bill 2575 and its corresponding bipartisan Senate Bill 3502 (the "AI in Government Act")—which would task federal agencies with exploring the implementation of AI in their functions and establishing an "AI Center of Excellence,"—were first introduced in September 2018, and reintroduced in May 2019.[35] The center would be directed to "study economic, policy, legal, and ethical challenges and implications related to the use of artificial intelligence by the Federal Government" and "establish best practices for identifying, assessing, and mitigating any bias on the basis of any classification protected under Federal non-discrimination laws or other negative unintended consequence stemming from the use of artificial intelligence systems."

One of the sponsors of the bill, Senator Brian Schatz (D-HI), stated that "[o]ur bill will bring agencies, industry, and others to the table to discuss government adoption of artificial intelligence and emerging technologies. We need a better understanding of the opportunities and challenges these technologies present for federal government use and this legislation would put us on the path to achieve that goal."[36] Although the bill is aimed at improving the implementation of AI by the federal government, there are likely to be opportunities for industry stakeholders to participate in discussions surrounding best practices.[37]

5. OMB Guidance for Federal Regulatory Agencies

The EO directed the Office of Management and Budget ("OMB") director, in coordination with the directors of the Office of Science and Technology Police, Domestic Policy Council, and National Economic Council, and in consultation with other relevant agencies and key stakeholders (as determined by OMB), to issue a memorandum to the heads of all agencies to "inform the development of regulatory and non regulatory approaches" to AI that "advance American innovation while upholding civil liberties, privacy, and American values" and consider ways to reduce barriers to the use of AI technologies in order to promote their innovative application. The White House Office of Science and Technology Policy further indicated in April 2019 that regulatory authority will be left to agencies to adjust to their sectors, but with high-level guidance from the OMB, as directed by the EO.[38]

In January 2020, the OMB published a draft memorandum featuring 10 "AI Principles" and outlining its proposed approach to regulatory guidance for the private sector which echoes the "light-touch" regulatory approach espoused by the 2019 EO, noting that promoting innovation and growth of AI is a "high priority" and that "fostering innovation and growth through forbearing from new regulations may be appropriate."[39] The guidance directs federal agencies to "avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth" and notes that in certain circumstances it may be appropriate to preempt "inconsistent, burdensome and duplicative State laws," although it also cautions that agencies should consider forgoing regulatory action where a "uniform national standard for a specific aspect related to AI is not essential."[40] As expected, the principles favor flexible regulatory frameworks that allow for rapid change and updates across sectors, rather than one-size-fits-all

regulations, and urge European lawmakers to avoid heavy regulation frameworks. The guidance encourages federal agencies to provide opportunities for public comment in AI rulemaking.

The principles also address some of the concerns raised by commentators with regard to ethics and particularly unwanted bias, urging lawmakers to consider whether the technology will "introduce real-world bias that produces discriminatory outcomes" and advising agencies to pursue transparency by disclosing the use of AI technology and making sure that outcomes are sufficiently transparent to ensure that the algorithms comply with existing laws.

6. National Security and Military Use

In the last few years, the US federal government has been very active in coordinating cross-agency leadership and planning for bolstering continued research and development of artificial intelligence technologies for use by the government itself. Along these lines, a principle focus for a number of key legislative and executive actions was the growth and development of such technologies for national security and military uses.

As a result of the passing of the John S. McCain National Defense Authorization Act for 2019 (the 2019 NDAA),[41] the National Security Commission on Artificial Intelligence was established to study current advancements in artificial intelligence and machine learning, and their potential application to national security and military uses. In addition, in response to the 2019 NDAA, the Department of Defense ("DoD") created the Joint Artificial Intelligence Center ("JAIC") as a vehicle for developing and executing an overall AI strategy, and named its director to oversee the coordination of this strategy for the military.[42] While these actions clearly indicate an interest in ensuring that advanced technologies like AI also benefit the US military and intelligence communities, the limited availability of funding from Congress may hinder the ability of these newly formed entities to fully accomplish their stated goals.

The JAIC is becoming the key focal point for the DoD in executing its overall AI strategy. As set out in a February 2019 summary of AI strategy provided by the DoD,[43] the JAIC will work with the Defense Advanced Research Projects Agency ("DARPA"),[44] various DoD laboratories, and other entities within the DoD to not only identify and deliver AI-enabled capabilities for national defense, but also to establish ethical guidelines for the development and use of AI by the military.[45] However, JAIC's efforts to be a leader in defining ethical uses of AI in military applications may prove challenging because one of the most hotly debated uses of AI is in connection with autonomous weaponry.[46] As this Review went to press, the White House released its 2021 budget request to Congress, which proposed a funding windfall for AI-related research and development, particularly in the military sector.[47]

On October 31, 2019, the Defense Innovation Board ("DIB"), an independent federal advisory committee to the Pentagon consisting of a group of science and technology experts—led by former Google CEO Eric Schmidt—proposed a new ethics framework consisting of five overarching ethical principles which tie the DoD existing laws of war and rules of engagement[48] into the use of AI.[49] The report is a high-level blueprint for military deployments of artificial intelligence and addresses some general shortcomings of AI technology.[50] The principles advocate for deliberate AI designs to counter

unintended biases that could cause inadvertent harm and for humans to have the power to deactivate or disengage AI systems acting outside the intended parameters. The DIB also suggested that humans should always be responsible for the "development, deployment, use and outcomes" of AI rather than letting AI set its own standards of use. In these cases, DoD should not use that AI system because "it does not achieve mission objectives in an ethical or responsible manner."[51]

The DIB also recommended a number of technical and organizational measures that would help lay the groundwork to ensure military artificial intelligence systems adhere to ethical standards, such as increasing investment in standards development, workforce programs and AI security applications, and formalizing channels for exploring the ethical implications of deploying AI technology across the department. The newly proposed ethics framework could help address private sector concerns about innovative technology being wrongly weaponized or misused by the military or being part of autonomous systems without sufficient human oversight.

a) The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update

Three years after the release of the initial National Artificial Intelligence Research and Development Strategic Plan, in June 2019 the Trump administration issued an update—previewed in the EO—bringing forward the original seven focus areas and adding an eighth: public-private partnerships.[52] The update highlights the benefits of strategically leveraging academic and industry expertise, including facilities, datasets, and expertise, to advance science and engineering innovations. Companies interested in exploring the possibility of individual collaborations or joint programs advancing precompetitive research should consider whether they have relevant expertise in any of the areas in which federal agencies are actively pursuing public-private partnerships, including the DoD's Defense Innovation Unit and the Department of Health and Human Services.[53]

b) NSCAI Report on U.S. National Security

On November 4, 2019, the National Security Commission on Artificial Intelligence ("NSCAI")—which was tasked by Congress to research ways to advance the development of AI for national security and defense purposes—released a highly anticipated interim report specifying five key areas in which U.S. policy can improve in order to transition AI from "a promising technological novelty into a mature technology integrated into core national security missions."[54] The commission worked with a number of U.S. government departments and agencies including the intelligence community, academia and the private sector, as well as allied partners such as the United Kingdom, Japan, Canada and Australia. Across all five principles, NSCAI said that ethical and responsible development and deployment of AI is a top priority, and noted that it is still developing best practices for operationalizing AI technologies that are trustworthy, explainable, and free of unwanted bias. The five lines of effort are: invest in research and development; apply the technology to national security missions; train and recruit AI talent; protect and build upon U.S. technology advantages; and marshal global cooperation on artificial intelligence issues.

The commission's preliminary conclusion is that the U.S. "is not translating broad national AI strengths and AI strategy statements into specific national security advantages."[55] Notably, the commission reported that federal R&D funding has not kept pace with the potential of AI technologies, noting that the requested fiscal year 2020 federal funding for core AI research outside of the defense sector grew by less than 2 percent from the estimated 2019 levels.[56] Further, it noted that AI is not realizing its potential to execute core national security missions because agencies are failing to embrace the technology as a result of "bureaucratic impediments and inertia."[57] NSCAI also criticized the shortage of AI talent in government agencies, specifically in the Department of Defense ("DoD"). It made workforce development recommendations to federal agencies, including undertaking more widespread use of AI technologies, and improving training on basic AI principles.[58] The commission asserted that the U.S. has a global technological advantage in terms of AI implementation, but also warned that China is rapidly closing the gap.[59] NSCAI recommended export controls to protect AI hardware,[60] and preservation of an open research system with U.S. academia. Finally, the commission said the U.S. should lead creation of AI norms worldwide by fostering international collaboration and establishing a network of allies dedicated to AI data sharing, R&D coordination, capacity building, and talent exchanges.

NSCAI is set to release its final report and recommendations—which will likely contain additional insights into U.S. federal policy regarding AI—in March 2021.

B. U.S. Imposes Export Controls Related to AI

On October 7, 2019, the Department of Commerce Bureau of Industry and Security ("BIS") announced that it will add 28 Chinese governmental and commercial organizations to the Entity List for engaging in or enabling activities contrary to the foreign policy interests of the United States.[61] The regulation includes China's leading AI companies, including Sense Time, Megvii Technology, Yitu, and Dahua Technology. Companies are required to comply with the notice as of the effective date, although it includes a standard "savings clause" exempting items that are already en route as of October 9, 2019. The Secretary of Commerce stated that this action was in response to "the brutal suppression of ethnic minorities within China[.]"[62]

On January 3, 2020, BIS also announced its first unilateral control on a specific application of AI in software that automates certain data analysis of geospatial imagery data.[63] The United States has previously imposed controls on certain enabling technologies for AI in concert with other countries that participate in multilateral export control regimes. However, this is the first new AI control imposed by BIS since it began evaluating potential controls on AI as one of among several types of emerging or foundational technologies pursuant to congressionally imposed mandate in the Export Control Reform Act of 2018.

While BIS has indicated in many public fora that it will strive to ensure that any new controls it may impose on emerging and foundational technologies like AI are also adopted in peer countries that participate in the Wassenaar Arrangement, among other multilateral export regimes, the development of international consensus around specific controls often requires years of outreach and negotiation. Likely due to the significant national security-related concerns associated with development of AI-enabled,

automated geospatial data analysis software, BIS opted to act unilaterally now. The specific software now subject to controls is described under Export Control Classification Number (ECCN) 0D521. Effective immediately, all exports of the software to countries worldwide (except Canada) and will now require an individual license from BIS. Moreover, releases of the software in source code to non-U.S. persons, for example, non-U.S. person employees, also require licensing. The only exception for the new license requirement is for exports of the software when transferred by or to a department or agency of the U.S. Government. In addition to these new licensing requirements, BIS's control of the software under the new ECCN makes the software a kind of critical technology for the purposes of foreign investment review by the Committee on Foreign Investment in the United States ("CFIUS").

III. EU POLICY & REGULATORY DEVELOPMENTS

In 2019, the European Union ("EU") announced that it was preparing comprehensive legislation to govern AI, took steps to demonstrate its commitment toward the advancement of AI technology through funding,[64] while simultaneously pressing for companies and governments to develop ethical applications of AI. As we have addressed previously,[65] given the stringent requirements of the European General Data Protection Regulation ("GDPR"), future EC regulations are likely to stand in contrast to the current U.S. "light-touch" regulatory approach and could have a significant impact on companies developing or operating AI products within the EU. Given that the U.S. and China currently lead the global AI race in terms of technological advancement, the "regulate-first" approach of the European Union ("EU") has led to concerns that it will impede innovation within the EU.[66]

A. EC Focus on Comprehensive AI Regulation

In mid-2019, the new president of the European Commission ("EC"), Ursula von der Leyen, unveiled her five-year policy agenda and promised to put forward legislation "for a coordinated European approach on the human and ethical implications of AI" by March 2020.[67]

In a speech at the European Parliament on November 27, 2019, von der Leyen said that she was in favor of AI-focused legislation similar to the GDPR.[68] The Commission is also likely to draw on the work of its high-level expert group on AI, which outlined a series of principles earlier this year aimed at ensuring companies deploy artificial intelligence in a way that is fair, safe and accountable. In January 2020, a leaked draft of a white paper noted that the EC was considering a five-year ban on the use of facial recognition technology in public spaces, although recent press reports indicate that the EC has since scrapped the possibility of a ban.[69] The draft also suggested that the EU's executive body is in fact leaning towards tweaks of existing rules and sector/application-specific risk assessments and requirements, rather than blanket sectoral requirements or bans.[70] The proposal also emphasizes the need for an oversight governance regime to ensure rules are followed—though the Commission suggested leaving Member States to choose whether to rely on existing governance bodies for this task or create new ones dedicated to regulating AI. The revised proposal, part of a package of measures to address the challenges of AI, could still be amended before the Commission presents its plan on February 19, 2020.

On the basis of these statements, we anticipate that the AI legislation will:

(1) be comprehensive and sweeping in nature, aiming to address fundamental questions at a more abstract level (similar to the GDPR);

(2) be focused on individual rights (including information rights) and require GDPR-style impact assessments to ensure AI systems do not perpetuate discrimination or violate fundamental rights;

(3) address government funding of research, workplace training and the availability of public data;

(4) require, like some U.S. states—notably California—that any chatbot or virtual assistant interacting with individuals will need to disclose that it is not a human, and create enhanced requirements for transparency as to the use of data and the bases for decisions or recommendations to avoid unintended bias or disparate impact; and

(5) contain rules for accountability, mitigation of bias and discrimination, liability and transparency throughout the entire life cycle of a product or service.[71]

The legislative initiative is part of a bigger effort to secure a competitive advantage and to increase public and private investment in AI to €20 billion per year.[72] A key challenge for the new president of the EC von der Leyen will be to grow investment, data, and talent required to develop AI and accelerate its adoption, and to create an innovation-friendly regulatory environment across the EU.

B. Ethics Guidelines for Trustworthy AI

Another focus of regulatory activity within the EU and individual EU Member States has been the development of ethical considerations in the use of AI. In connection with the implementation of the GDPR in 2018, in April 2019, the EC released a report from its "High-Level Expert Group on Artificial Intelligence" ("AI HLEG"): the EU "Ethics Guidelines for Trustworthy AI" ("Ethics Guidelines").[73] The Ethics 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, the Ethics Guidelines highlight the importance of implementing a "large-scale pilot with partners" and of "building international consensus for human-centric AI,"[74] and contain an "assessment list" which operationalizes the ethical principles and offers guidance to implement them in practice.[75] Along with the release of the Ethics Guidelines, the EC initiated a pilot phase of guideline implementation to assess the practical implementation of the assessment list and to gather feedback on how it can be improved.[76] Following the end of the piloting phase in December 2019, the AI HLEG will evaluate the feedback received and propose a revised version of the assessment list to the EC in early 2020.[77]

The EU also intends to "continue to play an active role in international discussions and initiatives including the G7 and G20."[78] 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 and therefore merits continued attention.

C. German Data Ethics Commission Report

On October 23, 2019, Germany's Data Ethics Commission ("Ethics Commission") released a landmark 240-page report containing 75 recommendations for regulating data, algorithmic systems and AI.[79] Consistent with EC President Ursula von der Leyen's recent remarks, the report suggests that EU regulation of AI may mirror the approach espoused in the GDPR—broad in scope, focused on individual rights and corporate accountability, and "horizontally" applicable across industries, rather than specific sectors.[80] Expanding on the EU's non-binding "Ethics Guidelines for Trustworthy AI," the commission concludes that "regulation is necessary, and cannot be replaced by ethical principles."[81]

The report creates a blueprint for the implementation of binding legal rules for AI—nominally both at national and EU level—on a sliding scale based on the risk of harm across five levels of algorithmic systems, with a focus on the degree of potential harm rather than differentiating between specific use cases. While systems posing a negligible or low likelihood of harm would not require any new regulatory obligations, those with at least "some" potential for harm would be subject to a mandatory labeling scheme that indicates where and how algorithms are being used within the system, and a risk assessment that evaluates the system's effect on privacy rights, self-determination, bodily or personal integrity, assets and ownership rights, and discrimination, among other factors. For systems that curate content based on user data, such as personalized pricing algorithms, the commission recommends prior authorization by supervisory institutions, and heightened oversight (such as live monitoring) and transparency obligations systems with "regular or significant potential for harm," which include determinations about consumer creditworthiness. The commission recommended a full or partial ban on systems with an "untenable potential for harm."[82]

Of particular relevance to companies deploying AI software, the Ethics Commission recommends that measures be taken against "ethically indefensible uses of data," such as "total surveillance, profiling that poses a threat to personal integrity, the targeted exploitation of vulnerabilities, addictive designs and dark patterns, methods of influencing political elections that are incompatible with the principle of democracy, vendor lock-in and systematic consumer detriment, and many practices that involve trading in personal data."[83] The Ethics Commission also recommends that human operators of algorithmic systems be held vicariously liable for any harm caused by autonomous technology, and calls for an overhaul of existing product liability and strict liability laws as they pertain to algorithmic products and services.[84]

While the report's pro-regulation approach is a counterweight to the "light-touch" regulation favored by the U.S. government, the Ethics Commission takes the view that, far from impeding private sector innovation, regulation can provide much-needed certainty to companies developing, testing, and deploying innovative AI products.[85] Certainly, the Ethics Commission's guiding principles—among them the need to ensure "the human-centred and value-oriented design of technology"[86]—reinforce that European lawmakers are likely to regulate AI development comprehensively and decisively. While it remains to be seen to what extent the forthcoming draft EU legislation will adopt the commission's recommendations, all signs point to a sweeping regulatory regime that could significantly impact technology companies active in the EU.

IV. REGULATION OF AI TECHNOLOGIES AND ALGORITHMS

As the use of AI expands into different sectors and the need for data multiplies, legislation that traditionally has not focused on AI is starting to have a growing impact on AI technology development. Defining and achieving an ethical approach to AI decision-making has been at the forefront of policy discussions relating to the private sector for some time, and the deep learning community has responded with a wave of investments and initiatives focusing on processes designed to assess and mitigate bias and disenfranchisement[87] at risk of becoming "baked in and scaled" by AI systems.[88] Such discussions are now becoming more urgent and nuanced with the increased availability of AI decision-making tools allowing government decisions to be delegated to algorithms to improve accuracy and drive objectivity, directly impacting democracy and governance.[89] Over the past year, we have seen those discussions evolve into tangible and impactful legislative proposals and concrete regulations in the data regulation space and, notably, several outright technology bans.[90]

A. Algorithmic Accountability

In 2019, a number of federal bills addressing algorithmic accountability and transparency hinted at a shift in Washington's stance amid growing public awareness of AI's potential to create bias or harm certain groups.[91] While the proposed legislation remains in its early stages, it is indicative of the government's increasingly bold engagement with technological innovation and the regulation of AI, and companies operating in this space should remain alert to both opportunities and risks arising out of federal legislative and policy developments—particularly the increasing availability of public-private partnerships—during 2020.

1. H.R. 153

In February 2019, the House introduced Resolution 153 , with the intent of "[s]upporting the development of guidelines for ethical development of artificial intelligence" and emphasizing the "far-reaching societal impacts of AI" as well as the need for AI's "safe, responsible, and democratic development."[92] Similar to California's adoption last year of the Asilomar Principles[93] and the OECD's recent adoption of five "democratic" AI principles,[94] the House Resolution provides that the guidelines must be consonant with certain specified goals, including "transparency and explainability," "information privacy and the protection of one's personal data," "accountability and oversight for all automated decisionmaking," and "access and fairness." This Resolution puts ethics at the forefront of policy, which differs from other legislation that considers ethics only as an ancillary topic. Yet, while this resolution signals a call to action by the government to come up with ethical guidelines for the use of AI technology, the details and scope of such ethical regulations remain unclear.

2. Algorithmic Accountability Act

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."[95] Rep. Yvette D. Clarke (D-NY) introduced a companion bill in the House.[96] 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 technology area. The bill reflects a step back from the previously favored approach of industry self-regulation, since it would force companies to actively monitor use of any potentially discriminatory algorithms. Although it does not provide for a private right of action or enforcement by state attorneys general, it would give the Federal Trade Commission the authority to enforce and regulate these audit procedures and requirements. Further congressional action on this subject can certainly be anticipated.

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."[97] 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[,]" "sensitives 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[.]"[98] 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. 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.

Although the bill still faces an uncertain future, if it is enacted, businesses would face a number of challenges, not least significant uncertainty in defining and, ultimately, seeking to comply with the proposed requirements for implementing "high risk" AI systems and utilizing consumer data, as well as the challenges of sufficiently explaining to the FTC the operation of their AI systems. Moreover, the bill expressly states that it does not preempt state law—and states that have already been developing their own consumer privacy protection laws would likely object to any attempts at federal preemption—potentially creating a complex patchwork of federal and state rules.[99] 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.

3. Bot Disclosure and Accountability Act (S. 2125)

The Bot Disclosure and Accountability Act, first introduced on June 25, 2018 and reintroduced on July 16, 2019, mandates that the FTC come up with regulations that force digital platforms to publicly disclose their use of an 'automated software program or process intended to replicate human activity online'.[100] It also prohibits political candidates or parties from using these automated software programs in order to share or disseminate any information targeting political elections. The Act hands the task of defining 'automated software program' to the FTC, which leaves wide latitude in interpretation beyond the narrow bot purpose for which the bill is intended.

At the state level, California passed a bill in September 2018, the 'Bolstering Online Transparency Act',[101] which was the first of its kind and (similar to the federal bot bill) is intended to combat malicious bots operating on digital platforms. This state law does not attempt to ban bots outright, but requires companies to disclose whether they are using a bot to communicate with the public on their internet platforms. The law went into effect on July 1, 2019.

4. Filter Bubble Transparency Act (S. 2763)

On October 31, 2019 a bipartisan group of senators introduced the Filter Bubble Transparency Act, the first substantive federal bill aimed at regulating algorithmic control of content on internet platforms. If enacted, the bill would require large-scale internet platforms to provide greater transparency to consumers by providing clear notice on the use, and enabling consumers to opt out, of personalized content curated by "opaque" algorithms so that they can "engage with a platform without being manipulated by algorithms driven by user-specific data"[102] and "simply opt out of the filter bubble."[103] "Filter bubble" refers to a zone of potential manipulation that exists within algorithms that curate or rank content in internet platforms based on user-specific data, potentially creating digital "echo chambers."[104]

The proposed legislation covers "any public-facing website, internet application, or mobile application," such as social network sites, video sharing services, search engines and content aggregation services,[105] and generally would prohibit the use of opaque algorithms on platforms without those platforms having first provided notice in a "clear, conspicuous manner on the platform whenever the user interacts with an opaque algorithm for the first time." The term "opaque algorithm" is defined as "an algorithmic ranking system[106] that determines the order or manner that information is furnished

to a user on a covered internet platform based, in whole or part, on user-specific data that was not expressly provided by the user to the platform" in order to interact with it.[107] Examples of "user-specific" data include the user's history of web searches and browsing, geographical locations, physical activity, device interaction, and financial transactions.[108] Conversely, data that was expressly provided to the platform by the user for the purpose of interacting with the platform—such as search terms, saved preferences, an explicitly entered geographical location or the user's social media profiles[109]—is considered "user-supplied."

Additionally, the bill requires that users be given the option to choose to view content based on "input-transparent algorithms," a purportedly generic algorithmic ranking system that "does not use the user-specific data of a user to determine the order or manner that information is furnished to such user on a covered platform,"[110] and be able to easily switch between the opaque and the input-transparent versions.[111] By way of example, Sen. Marsha Blackburn (R-TN), another co-sponsor of the bill, explained that "this legislation would give consumers the choice to decide whether they want to use the algorithm or view content in the order it was posted."[112] However, there is nothing in the bill that would require platforms to disclose the use of algorithms unless they are using hyper-personal "user-specific" data for customization, and even "input-transparent" algorithms using "user-supplied" data would not necessarily show content in chronological order. Nor would platforms be required to disclose any source code or explain how the algorithms used work. As drafted, the bill's goals of providing transparency and protecting consumers from algorithmic manipulation by "opting out" of personalized content appear to be overstated, and lawmakers will need to grapple with the proposed definitions to clarify the scope of the bill's provisions.[113]

Like the Algorithmic Accountability Act, the bill is squarely targeted at "Big Tech" platforms—it would not apply to platforms wholly owned, controlled and operated by a person that did not employ more than 500 employees in the past six months, averaged less than $50 million in annual gross receipts, and annually collects or processes personal data of less than a million individuals.[114] Violations of the Act would be enforced with civil penalties by the Federal Trade Commission ("FTC") but, unlike the Algorithmic Accountability Act, the bill does not grant state attorneys general the right to bring civil suits for violations, nor expressly state that its provisions do not preempt state laws.[115]

B. Facial Recognition Software

Biometric surveillance, or "facial recognition technology," has emerged as a lightning rod for public debate regarding the risk of improper algorithmic bias and data privacy concerns. Until recently, there were few if any laws or guidelines governing the use of facial recognition technology. Amid widespread fears that the current state of the technology is not sufficiently accurate or reliable to avoid discrimination, regulators have seized the opportunity to act in the AI space—proposing and passing outright bans on the use of facial recognition technology with no margin for discretion or use case testing while a broader regulatory approach develops and the technology evolves.[116] This tentative consensus stands in stark contrast to the generally permissive approach to the development of AI systems in the private sector to date. While much of the regulatory activity to date has been at the local level, momentum is also building for additional regulatory actions at both the state and federal levels.

1. Federal Regulation

The federal government has indicated a willingness to consider a nationwide ban on facial recognition technology, or at least to enact stringent regulations. A bill introduced in Congress in March 2019 (S. 847, "Commercial Facial Recognition Privacy Act of 2019") would ban users of commercial face recognition technology from collecting and sharing data for identifying or tracking consumers without their consent, although it does not address the government's uses of the technology.[117] With few exceptions, the bill would require facial recognition technology available online to be made accessible for independent third-party testing "for accuracy and bias." The bill remains pending and has been referred to the Committee on Commerce, Science, and Transportation.

Several other federal bills on facial recognition technology have been proposed. H.R. 3875 was introduced on July 22, 2019, to "prohibit Federal funding from being used for the purchase or use of facial recognition technology."[118] On July 25, 2019, Representatives Yvette Clark (D-NY), Ayanna Pressley (D-Mass.) and Rashida Tlaib (D-Mich.) introduced the "No Biometric Barriers to Housing Act." If passed, the bill would prohibit facial recognition in public housing units that receive Department of Housing and Urban Development ("HUD") funding. It would also require HUD to submit a report on facial recognition and its impacts on public housing units and tenants.[119] Also on July 25, 2019, the Facial, Analysis, Comparison, and Evaluation ("FACE") Protection Act of 2019 (H.R. 4021) was introduced to prohibit a federal agency from applying "facial recognition technology to any photo identification issued by a State or the Federal Government or any other photograph otherwise in the possession of a State or the Federal Government unless the agency has obtained a Federal court order determining that there is probable cause for the application of such technology."[120]

The House Committee on Oversight and Reform has held several hearings on transparency regarding government use cases, at which Committee members voiced strong bipartisan support for providing transparency and accountability to the use of facial recognition technology.[121] To date, the group is continuing to work on legislation that could regulate the use of facial recognition by the private sector, federal government, and law enforcement. On January 15, 2020, the House Oversight and Reform Committee held its third hearing in less than a year about facial recognition, this time to explore its use in the private sector.[122]

2. State and Local Regulations

In 2019, lawmakers in numerous states introduced bills to ban or delay the use of facial recognition technology by government agencies or the private sector. In September 2019, California lawmakers passed legislation (A.B. 1215) which places a three-year moratorium on any facial recognition technology used in police body cameras beginning January 1, 2020.[123] The bill by Assemblyman Phil Ting (D-San Francisco), which was co-sponsored by the ACLU, was signed into law by Governor Newsom on October 8, 2019.[124] Previously, the ACLU had run demonstrations using facial-recognition technology which falsely flagged 26 California lawmakers as matching arrest photos.[125]

The language of A.B. 1215 states that using biometric surveillance violates constitutional rights because it is the "functional equivalent" of requiring people to carry identification at all times.[126] The new law

further regulates the collection of personal information, sounds in California's concern for overly broad collection of information, and may influence modifications to the California Consumer Privacy Act 2018 ("CCPA") regarding facial recognition (such as A.B. 1281, which would require businesses to give conspicuous notices where facial recognition technology is employed).

Amid increasing public concern about the technology operating in public spaces, 2019 also saw a string of efforts by various cities in the U.S. to ban the use of facial recognition technology by law enforcement.[127] Oakland City Council passed an ordinance to ban its use by city police and other government departments, joining San Francisco, California and Somerville, Massachusetts who had already enacted similar bans.[128] Berkeley City Council also adopted a ban at a meeting in mid-October 2019.[129]

C. Deepfake technology

A new AI application called "deepfakes" is raising a set of challenging policy, technology, and legal issues. Deepfake technology is used to combine and superimpose existing images and videos onto source images or videos—creating new "synthetic" images or videos—by using a machine learning technique known as a generative adversarial network ("GAN"), a deep neural net architecture comprised of two nets, pitting one against the other (the "adversarial"). Since GANs can learn to mimic any distribution of data (images, music, speech, or text), the applications of deepfake technology are vast. Prompted by increased public concern over the potential impact of the technology on everything from cybersecurity to electoral manipulation, tentative federal bills intended to regulate deepfakes have emerged over the past several months, while state legislatures have already reacted by banning certain deepfake applications.[130]

1. Federal Regulatory Efforts

In September 2018, Reps. Adam Schiff (D-Calif.), Stephanie Murphy (D-Fla.) and Carlos Curbelo (R-Fla.) sent a letter to the Director of National Intelligence to warn of potential risks relating to deepfakes.[131] The lawmakers cautioned that "[d]eep fakes have the potential to disrupt every facet of our society and trigger dangerous international and domestic consequences . . . [a]s with any threat, our Intelligence Community must be prepared to combat deep fakes, be vigilant against them, and stand ready to protect our nation and the American people."[132] In the wake of a June 2019 hearing by the House Permanent Select Committee on Intelligence on the national security challenges of artificial intelligence, manipulated media, and deepfake technology, both the House and the Senate introduced legislation to regulate GANs. At present, however, the bills appear to do very little to restrict the use of deepfake technology, suggesting that Congress remains in "learning mode."

On July 9, 2019, Sen. Rob Portman (R-OH) introduced the "Deepfake Report Act" (S. 2065), which would require the Department of Homeland Security to submit five annual reports to Congress on the state of the "digital content forgery" technology and evaluate available methods of detecting and mitigating threats.[133] The reports will include assessments of how the technology can be used to harm national security as well as potential counter measures. The bill defines digital content forgery as "the use of emerging technologies, including artificial intelligence and machine learning techniques, to

fabricate or manipulate audio, visual, or text content with the intent to mislead." The bipartisan bill was passed in the Senate by unanimous consent on October 25 and is currently before the House Committee on Energy and Commerce, which is reviewing the same-named companion bill, H.R. 3600.[134]

In the House, H.R. 3230 ("Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act" or the "DEEPFAKES Act") was introduced by Rep. Clarke (D-NY-9) on June 12, 2019.[135] It would require any "advanced technological false personation record" to be digitally watermarked. The watermark would be required to "clearly identifying such record as containing altered audio or visual elements." The bill has been referred to the Subcommittee on Crime, Terrorism, and Homeland Security.

On September 17, 2019, Rep. Anthony Gonzalez (R-OH) introduced the "Identifying Outputs of Generative Adversarial Networks Act" (H.R. 4355), which would direct both the National Science Foundation and NIST to support research on deepfakes to accelerate the development of technologies that could help improve their detection, to issue a joint report on research opportunities with the private sector, and to consider the feasibility of ongoing public and private sector engagement to develop voluntary standards for the outputs of GANs or comparable technologies.[136]

2. State Regulatory Efforts

In the wake of a June 2019 hearing by the House Permanent Select Committee on Intelligence on the national security challenges of artificial intelligence, manipulated media, and deepfake technology, both the House and the Senate introduced legislation to regulate deepfakes.

While those bills remains pending, California has taken action to restrict the specific use of deepfakes to influence elections and non-consensual pornographic deepfakes. On October 3, 2019 California's Gov. Newsom signed a bill (A.B. 730) banning anyone "from distributing with actual malice materially deceptive audio or visual media of the candidate" within 60 days of an election with the intent to injure the candidate's reputation or deceive a voter into voting for or against the candidate.[137] This measure exempts print and online media and websites if that entity clearly discloses that the deepfake video or audio file is inaccurate or of questionable authenticity. On October 3, Gov. Newsom also signed a bill (A.B. 602) banning pornographic deepfakes made without consent of the person depicted, creating a private right of action.[138] The law excepts "[c]ommentary, criticism, or disclosure that is otherwise protected by the California Constitution or the United States Constitution."

These laws may signal state regulators' willingness to quickly regulate other controversial AI applications going forward. It will remain to be seen whether these laws will be challenged and whether they will pass constitutional muster. Regardless, the use and proliferation of deepfakes will likely face greater legal and regulatory scrutiny at both federal and state level going forward, and may impact technology platforms which permit users to upload, share or link content.

D. Autonomous Vehicles

1. Federal Developments

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 (H.R. 3388)[139] by voice vote in September 2017, but its companion bill (the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act (S. 1885)),[140] 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.[141] Federal regulation of autonomous vehicles ("AVs") has so far faltered in the new Congress, as SELF DRIVE Act and the AV START Act have not been re-introduced since expiring with the close of the 115th Congress.[142]

In 2019, federal lawmakers have demonstrated renewed interest in a comprehensive AV bill aimed at speeding up the adoption of autonomous vehicles and deploying a regulatory framework. In July 2019, the House Energy and Commerce Committee and Senate Commerce Committee sought stakeholder input from the self-driving car industry in order to draft a bipartisan and bicameral AV bill, prompting stakeholders to provide feedback to the committees on a variety of issues involving autonomous vehicles, including cybersecurity, privacy, disability access, and testing expansion.[143] Moreover, several federal agencies have announced proposed rulemaking to facilitate the integration of autonomous vehicles onto public roads. And while federal regulations are lagging behind, legislative activity at the state and local level is stepping up to advance integration of autonomous vehicles in the national transportation system and local infrastructure.

In the meantime, 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. In January 2020, the DoT published updated guidance for the regulation of the autonomous vehicle industry, "Ensuring American Leadership in Automated Vehicle Technologies" or "AV 4.0."[144] The guidance builds on the AV 3.0 guidance released in October 2018, which introduced guiding principles for AV innovation for all surface transportation modes, and described the DoT's strategy to address existing barriers to potential safety benefits and progress.[145] AV 4.0 includes 10 principles to protect consumers, promote markets and ensure a standardized federal approach to AVs. In line with previous guidance, the report promises to address legitimate public concerns about safety, security, and privacy without hampering innovation, relying strongly on the industry self-regulating. However, the report also reiterates traditional disclosure and compliance standards that companies leveraging emerging technology should continue to follow.

During 2019, several federal agencies announced proposed rule-making to facilitate the integration of autonomous vehicles onto public roads. In May 2019, in the wake of a petition filed by General Motors requesting temporary exemption from Federal Motor Vehicle Safety Standards (FMVSSs) which require manual controls or have requirements that are specific to a human driver,[146] NHTSA announced that it was seeking comments about the possibility of removing 'regulatory barriers' relating to the

introduction of automated vehicles in the United States.[147] It is likely that regulatory changes to testing procedures (including preprogrammed execution, simulation, use of external controls, use of a surrogate vehicle with human controls and technical documentation) and modifications to current FMVSSs (such as crashworthiness, crash avoidance and indicator standards) will be finalized in 2021.

2. State Developments

State regulatory activity has continued to accelerate, adding to the already complex patchwork of regulations that apply to companies manufacturing and testing autonomous vehicles. State regulations vary significantly, ranging from allowing testing under certain specific and confined conditions to the more extreme, which allow for testing and operating AVs with no human passenger behind the wheel. Recognizing that AVs and vehicles with semi-autonomous components are already being tested and deployed on roads amid legislative gridlock at the federal level, 44 states and the District of Columbia have enacted autonomous vehicle legislation. In 2019 alone, 25 new bills were enacted in 25 states, and a further 56 remain pending.[148] 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.[149]

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.[150] 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.[151]

On April 12, 2019, the California DMV published proposed autonomous vehicle regulations that allow the testing and deployment of autonomous motor trucks (delivery vehicles) weighing less than 10,001 pounds on California's public roads.[152] The DMV held a public hearing on May 30, 2019, at its headquarters in Sacramento to gather input and discuss the regulations. The DMV's regulations continue to exclude the autonomous testing or deployment of vehicles weighing more than 10,001 pounds. In the California legislature, two new bills related to autonomous vehicles were introduced: S.B. 59[153] would establish a working group on autonomous passenger vehicle policy development while S.B. 336[154] would require transit operators to ensure certain automated transit vehicles are staffed by employees.

On June 13, 2019, Florida Governor Ron DeSantis signed into law C.S./H.B. 311, which establishes a statewide statutory framework, permits fully automated vehicles to operate on public roads, and removes obstacles that hinder the development of self-driving cars.[155] In Oklahoma, Governor Kevin Stitt signed legislation (S.B. 365) restricting city and county governments from legislating autonomous vehicles, ensuring that such legislation would be entirely in the hands of state and federal lawmakers.[156] Pennsylvania, which last year passed legislation creating a commission on "highly

automated vehicles," has proposed a bill that would authorize the use of an autonomous shuttle vehicle on a route approved by the Pennsylvania Department of Transportation (H.B. 1078).[157]

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.

E. Data Privacy

While not strictly focused on artificial intelligence technologies, a number of state and federal developments in the area of data privacy are noteworthy, given the central importance of access to large quantities of data (often including personal and private data) to the successful development and operation of many AI systems.[158]

1. Voter Privacy Act of 2019

In July 2019, California Senator Dianne Feinstein introduced the Voter Privacy Act of 2019, which is currently before the Senate Committee on Rules and Administration.[159] As introduced, the Act will give voters certain rights with regard to their personal data collected in connection with voter information. In particular, the Act provides notice rights, rights of access, deletion rights, and rights to prohibit transfer or targeting through use of the data. The stated purpose of the Act is to put an end to the manipulation and misdirection of voters through the use of their personal data, and the Act would be monitored by the Federal Election Commission. Obviously, for companies collecting voter information as part of the data processed by AI systems, the Act could add a number of significant compliance requirements should it ultimately pass.

2. California Consumer Privacy Act ("CCPA")

A series of amendments to the California Consumer Privacy Act ("CCPA") were signed into effect by the Governor in early October.[160] Some of these amendments may prove significant to certain businesses; such as A.B. 25, which provides a one-year carve-out of the personal information of employees from personal information that would otherwise fall under the requirements of the CCPA. Similarly, A.B. 1355 creates a one-year carve-out of certain personal information that is collected as part of purely business-to-business communications, which may also help alleviate concerns about how to handle personal information necessarily acquired in a business context. In addition to the amendments, the California Attorney General's Office released a series of proposed regulations for implementing the requirements of the CCPA, and initiated a period in which they will solicit public comments before making any final changes putting the regulations into force and effect.[161] The proposed regulations generally set out guidance for how businesses should implement the notice provisions of the CCPA, procedural steps for implementing consumer rights provisions and data collection requirements, as well as provide some clarification of the CCPA's non-discrimination provisions. The CCPA has been described as one of the most stringent state privacy laws and will affect AI technologies that are driven by personal data and companies who utilize or develop such technologies.

3. California "Anti-Eavesdropping Act"

On May 29, 2019 the California State Assembly passed a bill (A.B. 1395) requiring manufacturers of ambient listening devices like smart speakers to receive consent from users before retaining voice recordings, and banning manufacturers from sharing command recordings with third parties. The bill is currently pending in the State Senate.[162]

F. Intellectual Property

Intellectual property issues related to AI have also been at the forefront of the new technology, as record numbers of U.S. patent applications involve a form of machine learning component. In January 2019, the United States Patent and Trademark Office ("USPTO") released revised guidance relating to subject matter eligibly for patents and on the application of 35 U.S.C. § 112 on computer implemented inventions. On the heels of that guidance, on August 27, 2019, the USPTO published a request for public comment on several patent-related issues regarding AI inventions.[163] The request for comment posed 12 questions covering several topics from "patent examination policy to whether new forms of intellectual property protection are needed." The questions included topics such whether patent laws, which contemplate only human inventors, should be amended to allow entities other than a human being to be considered an inventor.[164] The commenting period was extended until November 8, 2019, and many of the comments submitted argue that ownership of patent rights should remain reserved for only natural or juridical persons.[165]

On December 13, 2019, the World Intellectual Property Organization ("WIPO") published a draft issue paper on IP policy and AI, and requested comments on several areas of IP, including patents and data, and, similarly to the USPTO before it, with regard to issues of inventorship and ownership.[166] The commenting period is set to end on February 14, 2020.

G. Law Enforcement

Increasingly, algorithms are also being used at every stage of criminal proceedings, from gathering evidence to making sentencing and parole recommendations. H.R. 4368, the "Justice in Forensic Algorithms Act of 2019," was introduced in the House on September 17, 2019, would prohibit the use of trade secrets privileges to prevent defense access to the source code of proprietary algorithms used as evidence in criminal proceedings, and require that the Director of NIST establish a program to provide for the creation and maintenance of standards for the development and use of computational forensic software ("Computational Forensic Algorithm Standards") to protect due process rights.[167] The standards would address underlying scientific principles and methods, an assessment of disparate impact on the basis of demographic features such as race or gender, requirements for testing and validating the software and for publicly available documentation, and requirements for reports that are provided to defendants by the prosecution documenting the use and results of computational forensic software in individual cases (e.g., source code).[168]

Police departments often use predictive algorithms for various 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.[169] Private groups, localities, states, and Congress have reacted to

concerns fomented by AI applied to policing. In a paper released on February 13, 2019, 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,[170] calling into question the validity of predictive policing systems and other criminal risk-assessment tools that use training sets consisting of historical data.[171] 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."[172]

A Utah law (H.B. 57) requiring that law enforcement obtain a warrant before accessing any person's electronic data went into effect in May 2019.[173] The law reflects a legislative recognition of individual privacy rights, and we will continue to closely watch this space and the extent to which its approach may be replicated in other state legislatures. Other efforts have been more limited in scope and focused only on certain AI applications, like facial recognition.[174] Beyond policy and advocacy, some groups have turned to the courts. The majority of these efforts sound in FOIA attempts to understand how police may be using predictive systems to aid their work.[175]

H. Health Care

Unsurprisingly, the use of AI in healthcare draws some of the most exciting prospects and deepest trepidation, given potential risks.[176] As of yet, there are few regulations directed at AI in healthcare specifically, but regulators have recently acknowledged that existing frameworks for medical device approval are not well-suited to AI-related technologies. The US Food and Drug Administration ("FDA") has proposed a specific review framework for AI-related medical devices, intended to encourage a pathway for innovative and life-changing AI technologies, while maintaining the FDA's patient safety standards.

In April 2019, the FDA recently published a discussion paper – 'Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)'—offering that new framework for regulating health products using AI/machine learning ("AI/ML") software as a medical device ("SaMD"), and seeking comment.[177] The paper introduces that one of the primary benefits of using AI in an SaMD product is the ability of the product to continuously update in light of an infinite feed of real-world data. But the current review system for medical devices requires a pre-market review, and pre-market review of any modifications, depending on the significance of the modification.[178] If AI-based SaMDs are intended to constantly adjust, the FDA posits that many of these modifications will require pre-market review – a potentially unsustainable framework in its current form. The paper instead proposes an initial pre-market review for AI-related SaMDs that anticipates the expected changes, describes the methodology, and requires manufacturers to provide certain transparency and monitoring, as well as updates to the FDA about the changes that in fact resulted in accordance with the information provided in the initial review. Additional discussion and guidance is expected following the FDA's review of the comments.

I. Financial Services

As the adoption of AI technology in the U.S. continues across a wide range of industries and the public sector, legislators are increasingly making efforts to regulate applicable data standards at federal level. On May 9, 2019, Representative Maxine Waters (D-CA) announced that the House Committee on Financial Services would launch two task forces focused on financial technology ("fintech") and AI:[179] a task force on financial intelligence that will focus on the topics of regulating the fintech sector, and an AI task force that will focus on machine learning in financial services and regulation, emerging risks in algorithms and big data, combatting fraud and digital identification technologies, and the impact of automation on jobs in financial services.[180]

On September 24, 2019, H.R. 4476, the Financial Transparency Act of 2019, was reintroduced into Congress.[181] The bipartisan bill, which calls for the Treasury secretary to create uniform, machine-readable data standards for information reported to financial regulatory agencies,[182] has been referred to the Subcommittee on Commodity Exchanges, Energy, and Credit. By seeking to make information that is reported to financial regulatory agencies electronically searchable, the bill's supporters aim to "further enable the development of RegTech and Artificial Intelligence applications," "put the United States on a path towards building a comprehensive Standard Business Reporting program," and "harmonize and reduce the private sector's regulatory compliance burden, while enhancing transparency and accountability."[183]

J. Labor and Hiring

Amid the acceleration in the spread of AI and automated decision-making in the public and private sector, many U.S. and multinational companies have begun to use AI to streamline and introduce objectivity into their employment process.[184] While AI presents an opportunity to eliminate bias from the hiring process, it has also been seen to introduce bias because of inadequate data underlying and powering its algorithms. Legislators are taking action to recognize the potentially vast implications of AI technology on employment and employees' rights. As a result, 2019 saw tentative legislation at federal and state level take on an increased focus upon AI in employment and hiring.

1. AI JOBS Act of 2019

On 28 January 2019, the proposed AI JOBS Act of 2019 was introduced and, if enacted, would authorize the Department of Labor to work with businesses and education institutions in creating a report that analyses the future of AI and its impact on the American labor landscape.[185] Similar to H.R. 153, this bill indicates federal recognition of the threat the introduction of AI technology poses; however, there is no indication as to what actions the federal government might take in order to offer labor protection, and the bill has not progressed to date.

2. Workers' Right to Training Act (S. 2468)

On September 11, 2019, Sen. Brown (D-OH) introduced S. 2468, the "Workers' Right to Training Act," which would require employers to provide notice and training to employees whose jobs are in danger of being changed or replaced due to technology, and for other purposes.[186] "Technology" is defined in

the bill as including "automation, artificial intelligence, robotics, personal computing, information technology, and e-commerce."[187]

3. Illinois AI Video Interview Act

Employers have begun using AI-powered interview platforms—equipped with abilities such as sentiment analysis, facial recognition, video analytics, neural language processing, machine learning and speech recognition—that are capable of screening candidates against various parameters to assess competencies, experience and personality on the basis of hundreds of thousands of data points, and rank them against other candidates based on an "employability" score.[188] However, the lack of transparency resulting from the use of proprietary algorithms to hire and reject candidates has led to some regulatory pushback.

In May 2019, the Illinois legislature unanimously passed H.B. 2557 (the "Artificial Intelligence Video Interview Act"), which governs the use of AI by employers when hiring candidates.[189] State Rep. Jaime Andrade Jr. (D), who co-sponsored the bill, noted that spoken accents or cultural differences could end up improperly warping the results of a video interview, and that people who declined to sit for the assessment could be unfairly punished by not being considered for the job.[190] On August 9, 2019, Governor J.B. Pritzker signed the Act into law, effective January 1, 2020. Under the Act, an employer using videotaped interviews when filling a position in Illinois may use AI to analyze the interview footage only if the employer:

- Gives notice to the applicant that the videotaped interview may be analyzed using AI for purposes of evaluating the applicant's fitness for the position. (A Senate floor amendment removed from the bill a requirement for written notice.)
- Provides the applicant with an explanation of how the AI works and what characteristics it uses to evaluate applicants.
- Obtains consent from the applicant to use AI for an analysis of the video interview.
- Keeps video recordings confidential by sharing the videos only with persons whose expertise or technology is needed to evaluate the applicant, and destroying both the video and all copies within 30 days after an applicant requests such destruction.

Illinois employers using such software will need to carefully consider how they are addressing the risk of AI-driven bias in their current operations, and whether hiring practices fall under the scope of the new law, which does not define "artificial intelligence," what level of "explanation" is required, or whether it applies to employers seeking to fill a position in Illinois regardless of where the interview takes place. While the Illinois Act currently remains the only such law to date in the U.S., companies using automated technology in recruitment should expect that the increasing use of AI technology in recruitment is likely to lead to further regulatory proposals in due course.[191]

[1] Most AI is specific to particular domains and problems. A "general" AI can be thought of as one that can be applied to a wide variety of cross-domain activities and perform at the level of, or better than a human agent, or has the capacity to self-improve its general cognitive abilities similar to or beyond human capabilities.

[2] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, First Edition, IEEE, 2019, at 2, *available at* https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html.

[3] Michael Guihot, *Will we ever agree to just one set of rules on the ethical development of artificial intelligence?*, World Economic Forum (June 17, 2019), available at https://www.weforum.org/agenda/2019/06/will-we-ever-agree-to-just-one-set-of-rules-on-the-ethical-development-of-artificial-intelligence.

[4] OECD Legal Instruments, Recommendation of the Council on Artificial Intelligence (May 21, 2019), *available at* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[5] *See* http://www.oecd.org/going-digital/ai/oecd-aigo-membership-list.pdf for the full list.

[6] The recommendations also instruct the OECD's Committee on Digital Economy Policy ("CDEP") to monitor the implementation of the recommendations and report to the Council on its implementation, to develop practical guidance for implementation and to promote the OECD AI Policy Observatory, an interactive forum for exchanging information on AI policy and activities due to launch on February 27, 2020 that will include a live database of AI strategies and initiatives as well as certain AI metrics, measurements, policies and good practices. *See* OECD, *OECD AI Policy Observatory: A platform for AI information, evidence, and policy options* (Sept. 2019), *available at* https://www.oecd.org/going-digital/ai/about-the-oecd-ai-policy-observatory.pdf.

[7] Press release, *Canada and France work with international community to support the responsible use of artificial intelligence* (May 16, 2019), *available at* https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/05/23_cedrico_press_release_ia_canada.pdf.

[8] Tim Simonite, *The World Has a Plan to Rein in AI—but the US Doesn't Like It*, Wired (January 6, 2020), *available at* https://www.wired.com/story/world-plan-rein-ai-us-doesnt-like/

[9] *Supra* note 2, The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, at 2.

[10] *Id.*, at 17.

[11] *Id.*, at 4.

[12] *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.

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

[14] Alexandra Brzozowski, *No progress in UN talks on regulating lethal autonomous weapons*, Euractiv (Nov. 22, 2019), *available at* https://www.euractiv.com/section/global-europe/news/no-progress-in-un-talks-on-regulating-lethal-autonomous-weapons/.

[15] The only notable legislative proposal was the Fundamentally Understanding the Usability and Realistic Evolution of Artificial Intelligence Act of 2017, also known as the FUTURE of Artificial Intelligence Act, which did not aim to regulate AI directly, but instead proposed a Federal Advisory Committee on the Development and Implementation of Artificial Intelligence. The Act has not been re-introduced in the new Congress.

[16] 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/.

[17] 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/.

[18] For an in-depth analysis, please see our update President Trump Issues Executive Order on "Maintaining American Leadership in Artificial Intelligence."

[19] 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/.

[20] *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.

[21] *Supra* note 16, section 2(a) (directing 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.').

[22] *Id*., section 5 (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').

[23] The EO asks federal agencies to prioritize fellowship and training programs to prepare for changes relating to AI technologies and promoting science, technology, engineering and mathematics (STEM) education.

[24] In addition, the EO encourages federal agencies to work with other nations in AI development, but also to safeguard the country's AI resources against adversaries.

[25] NIST's indirect participation in the development of AI-related standards through the International Organization for Standardization (ISO) may prove to be an early bellwether for future developments.

[26] NIST, U.S. Leadership in AI: a Plan For Federal Engagement in Developing Technical Standards and Related Tools – Draft For Public Comment (July 2, 2019), available .

[27] For instance, the EO established an internal deadline for agencies to submit responsive plans and memoranda for 10 August 2019.

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

[29] *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.

[30] H.R. 2022, 116th Cong (2019). 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.

[31] 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/.

[32] S. 1558, 116th Cong (2019–2020).

[33] The bill also establishes the National AI Research and Development Initiative to identify and minimize 'inappropriate bias and data sets algorithms'. The requirement for NIST to identify metrics used to establish standards for evaluating AI algorithms and their effectiveness, as well as the quality of training data sets, may be of particular interest to businesses. Moreover, the bill requires the Department of Energy to create an AI research program, building state-of-the-art computing facilities that will be made available to private sector users on a cost-recovery basis.

[34] Press Release, Senator Martin Heinrich, *Heinrich, Portman, Schatz Propose National Strategy For Artificial Intelligence; Call For $2.2 Billion Investment In Education, Research & Development* (May 21, 2019), *available at* https://www.heinrich.senate.gov/press-releases/heinrich-portman-schatz-propose-national-strategy-for-artificial-intelligence-call-for-22-billion-investment-in-education-research-and-development.

[35] H.R. 2575, 116th Cong. (2019-2020); S. 3502 – AI in Government Act of 2018, 115th Cong. (2017-2018).

[36] Press Release, Senator Brian Schatz, *Schatz, Gardner Introduce Legislation To Improve Federal Government's Use Of Artificial Intelligence* (September 2019), *available at* https://www.schatz.senate.gov/press-releases/schatz-gardner-introduce-legislation-to-improve-federal-governments-use-of-artificial-intelligence; *see also* Tajha Chappellet-Lanier, *Artificial Intelligence in Government Act is back, with 'smart and effective' use on senators' minds* (May 8, 2019), *available at* https://www.fedscoop.com/artificial-intelligence-in-government-act-returns.

[37] Note that, 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. 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. 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, and are often unregulated and deployed without public knowledge. 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. The bills were reintroduced in the 2020 session and remain in Committee. SB 5527, Reg. Sess. 2019-2020 (Wash. 2020); HB-1655, Reg. Sess. 2010-2020 (Wash. 2020).

[38] *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/.

[39] Director of the Office of Management and Budget, *Guidance for Regulation of Artificial Intelligence Applications* (Jan. 7, 2020), *available at* https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

[40] *Id*., at 2-3.

[41] H.R. 5515, 115th Cong. (2019). *See* https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

[42] *See* Cronk, Terri Moon, *DoD Unveils Its Artificial Intelligence Strategy* (February 12, 2019) at https://www.defense.gov/Newsroom/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/. In particular, the JAIC director's duties include, among other things, developing plans for the adoption of artificial intelligence technologies by the military and working with private companies, universities and nonprofit research institutions toward that end.

[43] Summary of the 2019 Department of Defense Artificial Intelligence Strategy, Harnessing AI to Advance Our Security and Prosperity (https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AISTRATEGY.PDF).

[44] Another potentially significant effort is the work currently being performed under the direction of DARPA on developing explainable AI systems. See https://www.darpa.mil/program/explainable-artificial-intelligence. Because it can be difficult to understand exactly how a machine learning algorithm arrives at a particular conclusion or decision, some have referred to artificial intelligence as being a 'black box' that is opaque in its reasoning. However, a black box is not always an acceptable operating paradigm, particularly in the context of battlefield decisions, within which it will be important for human operators of AI-driven systems to understand why particular decisions are being made to ensure trust and appropriate oversight of critical decisions. As a result, DARPA has been encouraging the development of new technologies to explain and improve machine–human understanding and interaction. See also DARPA's 'AI Next Campaign' (https://www.darpa.mil/work-with-us/ai-next-campaign).

[45] *Id*. at 9. *See also id*. at 15 (the JAIC 'will articulate its vision and guiding principles for using AI in a lawful and ethical manner to promote our values'.); in addition, under the 2019 NDAA, one duty of the JAIC director is to develop legal and ethical guidelines for the use of AI systems. https://www.govinfo.gov/ content/pkg/BILLS-115hr5515enr/pdf/BILLS-115hr5515enr.pdf

[46] Calls for bans or at least limits on so-called 'killer robots' go back several years, and even provoked several thousand signatories, including many leading AI researchers, to the Future of Life Institute's pledge. *See* https://futureoflife.org/lethal-autonomous-weapons-pledge.

[47] Allocations across the National Science Foundation, the Department of Energy's Office of Science and the Defense Advanced Research Projects Agency and the Department of Defense's Joint AI Center reach a combined $1.724 billion — with portions of an additional $150 million allocation for the Department of Agriculture and the National Institutes of Health going to AI research. Note that the draft budget also proposes a cut of 19%, or $154 million, to NIST's $653 million budget. *See* https://www.sciencemag.org/news/2020/02/trump-s-2021-budget-drowns-science-agencies-red-ink-again.

[48] Such as the U.S. Constitution, international treaties and the Pentagon's Law of War.

[49] Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense* (Oct. 31, 2019), *available at* https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

[50] Jack Corrigan, *Defense Innovation Board Lays Out 5 Key Principles for Ethical AI*, Nextgov (Oct. 31, 2019), *available at* https://www.nextgov.com/emerging-tech/2019/10/defense-innovation-board-lays-out-5-key-principles-ethical-ai/161008/.

[51] Daniel Wilson, *New Ethics Framework May Draw AI Firms To DOD*, Law360 (Nov. 8, 2019), *available at* https://www.law360.com/articles/1217965/new-ethics-framework-may-draw-ai-firms-to-dod.

[52] Exec. Office of the U.S. President, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* (June 2019), *available at* https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf, The updated plan also highlights what progress federal agencies have made with respect to the original seven focus areas: make long-term investments in AI research; develop effective methods for human-AI collaboration; understand and address the ethical, legal and societal implications of AI; ensure the safety and security of AI systems; develop shared public datasets and environments for AI training and testing; measure and evaluate AI technologies through standards and benchmarks; and better understand the national AI R&D workforce needs.

[53] *Id.*, at 42.

[54] National Security Commission on Artificial Intelligence, *Interim Report* (Nov. 2019), *available at* https://www.epic.org/foia/epic-v-ai-commission/AI-Commission-Interim-Report-Nov-2019.pdf

[55] *Id.*, at 22.

[56] *Id.*, at 25.

[57] *Id.*, at 31.

[58] *Id.*, at 36.

[59] *Id.*, at 18.

[60] *Id.*, at 41&44.

[61] U.S. Department of Commerce, Press Release, *U.S. Department of Commerce Adds 28 Chinese Organizations to its Entity List* (Oct. 7, 2019), *available at* https://www.commerce.gov/news/press-releases/2019/10/us-department-commerce-adds-28-chinese-organizations-its-entity-list.

[62] Anna Swanson and Paul Mozur, *U.S. Blacklists 28 Chinese Entities Over Abuses in Xinjiang*, N.Y. Times (Oct. 7, 2019), *available at* https://www.nytimes.com/2019/10/07/us/politics/us-to-blacklist-28-chinese-entities-over-abuses-in-xinjiang.html.

[63] U.S. Federal Register, Addition of Software Specially Designed To Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series (Docket No. BIS-2019-

0031) (Jan. 6, 2020), *available at* https://www.federalregister.gov/documents/2020/01/06/2019-27649/addition-of-software-specially-designed-to-automate-the-analysis-of-geospatial-imagery-to-the-export.

[64] The European Commission (EC) enacted a proposal titled: 'The Communication From the Commission to the European Parliament, the European Council, the European Economic and Social Committee, and the Committee of the Regions: Artificial Intelligence for Europe' (25 April 2018), https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe. The Communication set out the following regulatory proposals for AI: calls for new funding, pledges for investment in explainable AI 'beyond 2020', plans for evaluation of AI regulation, proposes that the Commission will support the use of AI in the justice system, pledges to draft AI ethics guidelines by the end of the year, proposes dedicated retraining schemes, and calls for prompt adoption of the proposed ePrivacy Regulation. Likewise, an April 2018 UK Select Committee Report on AI encouraged the UK government to establish a national AI strategy and proposed an 'AI Code' with five principles, emphasizing ideals such as fairness and developing for the common good – mirroring the EU's AI Ethics Guidelines. 'AI Policy – United Kingdom,' available at https://futureoflife.org/ai-policy-united-kingdom/?cn-reloaded=1.

[65] H. Mark Lyon, *Gearing Up For The EU's Next Regulatory Push: AI*, LA & SF Daily Journal (Oct. 11, 2019), *available at* https://www.gibsondunn.com/wp-content/uploads/2019/10/Lyon-Gearing-up-for-the-EUs-next-regulatory-push-AI-Daily-Journal-10-11-2019.pdf.

[66] *See further*, Ahmed Baladi, *Can GDPR hinder AI made in Europe?*, Cybersecurity Law Report (July 10, 2019), *available at* https://www.gibsondunn.com/can-gdpr-hinder-ai-made-in-europe/.

[67] Ursula von der Leyen, *A Union that strives for more: My agenda for Europe*, available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf. Note that the von der Leyen commission was slated to begin on November 1, 2019, but due to problems with filling three of the commissioners' seats, it was delayed until December 1, 2019 (thus pushing back the 100-day deadline).

[68] Oscar Williams, *New European Commission president pledges GDPR-style AI legislation*, New Statesman (Nov. 28, 2019), *available at* https://tech.newstatesman.com/policy/ursula-von-der-leyen-ai-legislation.

[69] Reuters, *EU Drops Idea of Facial Recognition Ban in Public Areas*, N.Y. Times (Jan. 30, 2020), available at https://www.nytimes.com/reuters/2020/01/30/technology/29reuters-eu-ai.html.

[70] European Commission, Structure for the white paper on Artificial Intelligence, Euractiv (Jan. 2, 2020), *available at* https://www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf.

[71] *See further*, H. Mark Lyon, *Gearing up for the EU's next regulatory push: AI*, LA & SF Daily Journal (Oct. 11, 2019), *available at* https://www.gibsondunn.com/wp-content/uploads/2019/10/Lyon-Gearing-up-for-the-EUs-next-regulatory-push-AI-Daily-Journal-10-11-2019.pdf.

[72] EC, *Artificial Intelligence for Europe*, COM(2018) 237 (Apr. 25, 2018), *available at* https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

[73] AI HLEG, *Ethics Guidelines for Trustworthy AI*, Guidelines (Apr. 8, 2019), *available at* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

[74] In a speech at the European Parliament on November 27, 2019, von der Leyen said that she was in favor of AI-focused legislation similar to the GDPR. The Commission is also likely to draw on the work of its high-level expert group on AI, which outlined a series of principles earlier this year aimed at ensuring companies deploy artificial intelligence in a way that is fair, safe and accountable. In a keynote speech at the World Economic Forum on January 22, 2020, von der Leyen stated that the GDPR had already set a pattern for the world and that the EU would "have to set a similar frame for artificial intelligence, too."

[75] AI HLEG, *Trustworthy AI Assessment List*, List (Apr. 8, 2019), *available at* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60440.

[76] EC, *Pilot the Assessment List of the Ethics Guidelines for Trustworthy AI*, website article *available at* https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/register-piloting-process-0.

[77] *Id.*

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

[79] German Federal Ministry for Justice and Consumer Protection, *Opinion of the Data Ethics Commission, Executive Summary* (October 2019), *available at* http://bit.ly/373RGqI.

[80] Jeremy Feigelson, Jim Pastore, Anna Gressel and Friedrich Popp, *German Report May Be Road Map For Future AI Regulation*, Law360 (Nov. 12, 2019), *available at* https://www.law360.com/articles/1218560/german-report-may-be-road-map-for-future-ai-regulation.

[81] German Federal Ministry for Justice and Consumer Protection, Opinion of the Data Ethics Commission, *supra*, note 33 at 7.

[82] *Id.*, at 19-20.

[83] *Id.*, at 10.

[84] *Id.*, at 26.

[85] David Meyer, *A.I. Regulation Is Coming Soon. Here's What the Future May Hold*, Fortune (Oct. 24, 2019), available at https://fortune.com/2019/10/24/german-eu-data-ethics-ai-regulation/.

[86] German Federal Ministry for Justice and Consumer Protection, Opinion of the Data Ethics Commission, *supra*, note 33 at 5.

[87] *See also* Kalev Leetaru, *Why Do We Fix AI Bias But Ignore Accessibility Bias?*, Forbes (July 6, 2019), *available at* https://www.forbes.com/sites/kalevleetaru/2019/07/06/why-do-we-fix-ai-bias-but-ignore-accessibility-bias/#55e7c777902d; Alina Tugend, *Exposing the Bias Embedded in Tech*, N.Y. Times (June 17, 2019), *available at* https://www.nytimes.com/2019/06/17/business/artificial-intelligence-bias-tech.html.

[88] Jake Silberg & James Manyika, *Tackling Bias in Artificial Intelligence (and in Humans)*, McKinsey Global Institute (June 2019), *available at* https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans.

[89] Nicol Turner Lee, Paul Resnick & Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, Brookings Institute (May 22, 2019), *available at* https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

[90] *See also* the French government's recent law, encoded in Article 33 of the Justice Reform Act, prohibiting anyone—especially legal tech companies focused on litigation prediction and analytics—from publicly revealing the pattern of judges' behavior in relation to court decisions, *France Bans Judge Analytics, 5 Years In Prison For Rule Breakers*, Artificial Lawyer (June 4, 2019), *available at* https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/.

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

[92] H.R. Res. 153, 116th Cong. (1st Sess. 2019).

[93] Assemb. Con. Res. 215, Reg. Sess. 2018-2019 (Cal. 2018) (enacted) (expressing the support of the legislature for the "Asilomar AI Principles"—a set of 23 principles developed through a collaboration between AI researchers, economists, legal scholars, ethicists and philosophers that met in Asilomar, California in January 2017 and categorized into "research issues," "ethics and values," and "longer-term issues" designed to promote the safe and beneficial development of AI—as "guiding values for the development of artificial intelligence and of related public policy").

[94] OECD Principles on AI (May 22, 2019) (stating that AI systems should benefit people, be inclusive, transparent, and safe, and their creators should be accountable), available at http://www.oecd.org/going-digital/ai/principles/.

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

[96] H.R. Res. 2231, 116th Cong. (1st Sess. 2019).

[97] *Supra*, note 66.

[98] *Id.*

[99] *See* Byungkwon Lim et al., *A Glimpse into the Potential Future of AI Regulation*, Law360 (April 10, 2019), *available at* https://www.law360.com/articles/1158677/a-glimpse-into-the-potential-future-of-ai-regulation.

[100] S.3127 – Bot Disclosure and Accountability Act of 2018, 115th Cong (2018), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/3127 and S.2125 Bot Disclosure and Accountability Act of 2019, 116th Cong (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2125.

[101] SB 1001, Bolstering Online Transparency Act (CA 2017), available at https://leginfo.legislature.ca.gov/faces/

billTextClient.xhtml?bill_id=201720180SB1001. We previously provided a detailed analysis of the new law in our client alert New California Security of Connected Devices Law and CCPA Amendments.

[102] Filter Bubble Transparency Act, S. 2763, 116th Cong. (2019). The bill's sponsors are Senators Marsha Blackburn (R-Tenn.), John Thune (R-S.D.), Richard Blumenthal (D-Conn.), Jerry Moran (R-Kan.)—all members of the Senate Committee on Commerce, Science, and Transportation, which has jurisdiction over the internet and consumer protection—and Mark Warner (D-Va.).

[103] Blackburn Joins Thune on Bipartisan Bill to Increase Internet Platform Transparency & Provide Consumers with Greater Control Over Digital Content, Marsha Blackburn, U.S. Senator for Tennessee (Oct. 31, 2019), https://www.blackburn.senate.gov/blackburn-joins-thune-bipartisan-bill-increase-internet-platform-transparency-provide-consumers.

[104] *Supra*, note 74; *see also* Zoe Schiffer, *'Filter Bubble' author Eli Pariser on why we need publicly owned social networks*, The Verge (Nov. 12, 2019), *available at* https://www.theverge.com/2019/11/5/20943634/senate-filter-bubble-transparency-act-algorithm-personalization-targeting-bill.

[105] Filter Bubble Transparency Act, *supra* n.1, at 2(4)(A)–(B). The bill provides that it is also applicable to common carriers that are subject to the Communications Act of 1934 and to "organizations not organized to carry on business for their own profit or that of their members." *Id.* at 4(B)(3).

[106] *Id.* at 2(B). The term "algorithmic ranking system" is broadly defined and encompasses any computational process—including "one derived from algorithmic decision-making, machine learning, statistical analysis, or other data processing or artificial intelligence techniques"—that is used to determine the order in which a set of information is provided to a user on a covered internet platform. Examples include "the ranking of search results, the provision of content recommendations, the display of social media posts, or any other method of automated content selection."

[107] Filter Bubble Transparency Act, *supra* n.1, at 2(1).

[108] *See id.* at 2(5)(B).

[109] *Id.* at 5(A), (C).

[110] *Id.* at 5(A).

[111] *Id.* at 3(A)–(B) (emphasis added).

[112] *Supra*, note 74.

[113] Adi Robertson, *The Senate's secret algorithms bill doesn't actually fight secret algorithms*, The Verge (Nov. 5, 2019), *available at* https://www.theverge.com/2019/11/5/20943634/senate-filter-bubble-transparency-act-algorithm-personalization-targeting-bill.

[114] The bill also exempts platforms that are operated for the sole purpose of conducting research that is not made for direct or indirect profit. *Id.* at 2(4)(A)–(B). Moreover, the bill does not cover contractors and subcontractors that receive rights to access indexes of web pages on the internet for the purpose of operating an internet search engine (i.e., downstream providers) from the respective upstream providers if "the search engine is operated by a downstream provider with fewer than 1,000 employees" and "the search engine uses an index of web pages on the internet to which such provider received access under a search syndication contract." *Id.* at 3(B)(2).

[115] On May 20, 2019, New Jersey introduced a similar bill, New Jersey Algorithmic Accountability Act (A.B. 5430), which requires covered entities to conduct impact assessments on "high-risk" automated decisions systems and information systems. New Jersey Algorithmic Accountability Act, A.B. 5430, 218th Leg., 2019 Reg. Sess. (N.J. 2019).

[116] U.S. H.R. Comm. on Oversight and Reform, Facial Recognition Technology (Part II): Ensuring Transparency in Government Use (June 4, 2019), *available at* https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-ii-ensuring-transparency-in-government-use.

[117] S. 847, 116th Cong. (1st Sess. 2019).

[118] H.R. 3875, 116th Cong. (2019).

[119] H.R. 4008, 116th Cong. (2019).

[120] FACE Protection Act of 2019, H.R. 4021, 116th Cong. (2019).

[121] U.S. H.R. Comm. on Oversight and Reform, Facial Recognition Technology (Part II): Ensuring Transparency in Government Use (June 4, 2019), *available at* https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-ii-ensuring-transparency-in-government-use.

[122] Khari Johnson, *Congress moves towards facial recognition regulation*, Venture Beat (Jan. 15, 2020), *available at* https://venturebeat.com/2020/01/15/congress-moves-toward-facial-recognition-regulation/.

[123] A.B. 1215 2019–2020 Reg. Sess. (Cal. 2019); *see also* Anita Chabria, *California could soon ban facial recognition technology on police body cameras* (Sept. 12, 2019), *available at* https://www.latimes.com/california/story/2019-09-12/facial-recognition-police-body-cameras-california-legislation.

[124] A.B. 1215 2019-2020 Reg. Sess. (Cal. 2019).

[125] *Id.*, at 44.

[126] *Id.*, at 1(c).

[127] *See* San Francisco Ordinance No. 103-19, the 'Stop Secret Surveillance' ordinance, effective 31 May 2019 (banning the use of facial recognition software by public departments within San Francisco, California); Somerville Ordinance No. 2019-16, the 'Face Surveillance Full Ban Ordinance', effective 27 June 2019 (banning use of facial recognition by the City of Somerville, Massachusetts or any of its officials); Oakland Ordinance No. 18-1891, 'Ordinance Amending Oakland Municipal Code Chapter 9.65 to Prohibit the City of Oakland from Acquiring and/or Using Real-Time Face Recognition Technology', preliminary approval 16 July 2019, final approval 17 September 2019 (bans use by city of Oakland, California and public officials of real-time facial recognition); Proposed Amendment attached to Cambridge Policy Order POR 2019 #255, approved on 30 July 2019 for review by Public Safety Committee (proposing ban on use of facial recognition technology by City of Cambridge, Massachusetts or any City staff); Attachment 5 to Berkeley Action Calendar for 11 June 2019, 'Amending Berkeley Municipal Code Chapter 2.99 to Prohibit City Use of Face Recognition Technology', voted for review by Public Safety Committee on 11 June 2019 and voted for continued review by Public Safety Committee on 17 July 2019 (proposing ban on use of facial recognition technology by staff and City of Berkeley, California). All of these ordinances incorporated an outright ban of use of facial recognition technology, regardless of the actual form or application of such technology. For a view on how such a reactionary ban is an inappropriate way to regulate AI

technologies, *see* Lyon, H Mark, 'Before We Regulate', Daily Journal (26 June 2019) available at https://www.gibsondunn.com/before-we-regulate.

[128] Sarah Ravani, *Oakland bans use of facial recognition technology, citing bias concerns*, SF Chronicle (July 17, 2019), *available at* https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php; *see also*, Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, N.Y. Times (July 13, 2019), *available at* https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

[129] Levi Sumagaysay, *Berkeley bans facial recognition*, Mercury News (Oct. 16, 2019), *available at* https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/.

[130] AB 730, AB 602 (California); SB 751 (Texas); HB 2678 (Virginia); HR 3230, 116th Congress (U.S. House of Representatives); S 2065, 116th Congress (U.S. Senate).

[131] Letter from Adam Schiff, U.S. Representative, Stephanie Murphy, U.S. Representative & Carlos Curbelo, U.S. Representative to Hon. Daniel R. Coats, Dir. of Nat'l Intelligence (Sept. 13, 2018).

[132] *Id.*

[133] S. 2065, 116th Congress (U.S. Senate).

[134] H.R. 3600, 116th Congress (U.S. House of Representatives).

[135] H.R. 3230, 116th Congress (U.S. House of Representatives).

[136] H.R. 4355, 116th Congress (U.S. House of Representatives).

[137] A.B. 730 2019–2020 Reg. Sess. (Cal. 2019).

[138] A.B. 602 2019-2020 Reg. Sess. (Cal. 2019).

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

[140] 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.

[141] 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.

[142] 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.

[143] Makena Kelly, *Congress wants the self-driving car industry's help to draft a new AV bill*, The Verge (July 31, 2019), *available at* https://www.theverge.com/2019/7/31/20748582/congress-self-driving-cars-bill-energy-commerce-senate-regulation.

[144] U.S. Dep't of Transp., *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0* (Jan. 2020), *available at* https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf.

[145] U.S. Dep't 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 further* our Artificial Intelligence and Autonomous Systems Legal Update (4Q18).

[146] General Motors, *LLC-Receipt of Petition for Temporary Exemption from Various Requirements of the Safety Standards for an All Electric Vehicle with an Automated Driving System*, 84 Fed. Reg. 10182.

[147] Docket No. NHTSA-2019-0036, 'Removing Regulatory Barriers for Vehicles With Automated Driving Systems', 84 Fed Reg 24,433 (28 May 2019) (to be codified at 49 CFR 571); see also 'Removing Regulatory Barriers for Vehicles with Automated Driving Systems', 83 Fed Reg 2607, 2607 (proposed 5 March 2018) (to be codified at 49 CFR 571). Thus far, the comments submitted generally support GM's petition for temporary exemption and the removal of regulatory barriers to the compliance certification of ADS-DVs. Some commentators have raised concerns that there is insufficient information in the petition to establish safety equivalence between traditionally operated vehicles and ADS-DVs, and regarding the ability of ADS-DVs to safely operate in unexpected and emergency situations. However, it is likely that NHTSA will grant petitions for temporary exemption to facilitate the development of ADS technology, contingent on extensive data-sharing requirements and a narrow geographic scope of operation. In addition, the Federal Motor Carrier Safety Administration also issued a request for comments on proposed rule-making for Federal Motor Carrier Safety Regulations that may need to be reconsidered for Automated Driving System- Dedicated Vehicles (ADS-DVs). Docket No. FMCSA-2018-0037. Safe Integration of Automated Driving Systems-Equipped Commercial Motor Vehicles, 84 Fed Reg 24,449 (28 May 2019).

[148] Nat'l Conference of State Legislatures, Autonomous Vehicles State Bill Tracking Database (Jan. 5, 2020), *available at* http://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx.

[149] 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.

[150] Andrew Glambrone, *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.

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

[152] State of California Department of Motor Vehicles, Autonomous Light-Duty Motor Trucks (Delivery Vehicles), *available at* https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/bkgd.

[153] S.B. 59, 2019–2020 Reg. Sess. (Cal. 2019).

[154] S.B. 336, 2019–2020 Reg. Sess. (Cal. 2019).

[155] Governor Ron DeSantis Signs CS/HB 311: Autonomous Vehicles (June 13, 2019), *available* at https://www.flgov.com/2019/06/13/governor-ron-desantis-signs-cs-hb-311-autonomous-vehicles/.

[156] S.B. 365, 57th Leg., Reg. Sess. (Okla. 2019).

[157] H.B. 1078, 2019–2020 Reg. Sess. (Pa. 2019).

[158] In addition to the legislation referenced in this section, and as we discuss in more detail in our U.S. Cybersecurity and Data Privacy Outlook and Review – 2020, litigation also continued around Illinois' Biometric Information Privacy Act ("BIPA"), including litigation predicated on the use of facial recognition technology.

[159] *See* S. 2398, 116th Congress (Senate).

[160] For more information, see our prior client alert, California Consumer Privacy Act: 2019 Final Amendments Signed, *available at* https://www.gibsondunn.com/california-consumer-privacy-act-2019-final-amendments-signed/.

[161] Again, for more information on the proposed regulations for CCPA, please see our prior client alert, California Consumer Privacy Act Update: Regulatory Update, *available at* https://www.gibsondunn.com/california-consumer-privacy-act-update-regulatory-update/.

[162] A.B. 1395, 2019–2010 Reg. Sess. (Cal. 2019).

[163] Request for Comments on Patenting Artificial Intelligence Inventions, 84 Fed. Reg. 44889, 44889 (Aug. 27, 2019); *see also* our client alert USPTO Requests Public Comments on Patenting Artificial Intelligence Inventions.

[164] *See further* Mark Lyon, Alison Watkins and Ryan Iwahashi, *When AI Creates IP: Inventorship Issues To Consider*, Law360 (Aug. 10, 2017), *available at* https://www.law360.com/articles/950313?scroll=1&related=1.

[165] Ryan Davis, *Law Shouldn't Let AI Be An Inventor On Patents, USPTO Told*, Law360 (Nov. 13, 2019), *available at* https://www.law360.com/articles/1218939/law-shouldn-t-let-ai-be-an-inventor-on-patents-uspto-told.

[166] WIPO Begins Public Consultation Process on Artificial Intelligence and Intellectual Property Policy, Press Release (Dec. 13, 2019), *available at* https://www.wipo.int/pressroom/en/articles/2019/article_0017.html.

[167] H.R. 4368, 116th Congress (U.S. House of Representatives).

[168] Press Release, *Rep. Takano Introduces the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System* (Sept. 17, 2019), *available at* https://takano.house.gov/newsroom/press-releases/rep-takano-introduces-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system.

[169] 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/.

[170] *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/.

[171] Meredith Whittaker, et al, *AI Now Report 2018*, AI Now Institute, 2.2.1 (December 2018), available at https://ainowinstitute.org/AI_Now_2018_Report; *see also* Rashida Richardson Schultz, Jason Schultz, and Kate Crawford, *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.

[172] Meredith Whittaker, et al, *AI Now Report 2018*, AI Now Institute, 2.2.1 (December 2018), available at https://ainowinstitute.org/AI_Now_2018_Report

[173] H.B. 2557, 2019-2010 Reg. Sess. (Ill. 2019) (101st Gen. Assembly).

[174] *See, e.g.*, A.B. 1215 2019–2020 Reg. Sess. (Cal. 2019); *see also* Anita Chabria, *California could soon ban facial recognition technology on police body cameras* (Sept. 12, 2019), *available at* https://www.latimes.com/california/story/2019-09-12/facial-recognition-police-body-cameras-california-legislation.

[175] *See, e.g., Stop LAPD Spying Coalition v. City of Los Angeles*, BS172216 (Cal. Super. Ct. 2018) – currently pending.

[176] For example, AI has been used in robot-assisted surgery in select fields for years, and studies have shown that AI-assisted procedures can result in far fewer complications. Brian Kalis, Matt Collier and Richard Fu, '10 Promising AI Applications in Health Care', Harvard Business Review (10 May 2018), available at https://hbr.org/2018/05/10-promising-ai-applications-in-health-care. Yet, The New York Times published an article in March 2019 warning of healthcare AI's potential failures, including

small changes in vernacular leading to vastly disparate results (eg, 'alcohol abuse' leading to a different diagnosis than 'alcohol dependence'); see Cade Metz and Craig S Smith, 'Warning of a Dark Side to A.I. in Health Care', The New York Times (21 March 2019), available at nytimes.com/2019/03/21/science/health-medicine-artificial-intelligence.html. And these issues are backed by studies, including one released by Science – one of the highest acclaimed journals – just prior to the article, which discusses how 'vulnerabilities allow a small, carefully designed change in how inputs are presented to a system to completely alter its outputs, causing it to confidently arrive at manifestly wrong conclusions.' Samuel G Finlayson, et al, 'Adversarial attacks on medical machine learning', SCIENCE 363:6433, pp. 1287–1289 (22 March 2019) *See* https://science.sciencemag.org/content/363/6433/1287.

[177] U.S. Food & Drug Administration, Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD), at 2 (2 April 2019), available at https://www.fda.gov/media/122535/download.

[178] The paper mentions that AI-based SaMDs have been approved by the FDA, but they are generally 'locked' algorithms, and any changes would be expected to go through pre-market review. This proposal attempts to anticipate continuously-adapting AI-based SaMD products.

[179] Katie Grzechnik Neill, *Rep. Waters Announces Task Forces on Fintech and Artificial Intelligence* (May 13, 2019), *available at* https://www.insidearm.com/news/00045030-rep-waters-announces-all-democrat-task-fo.

[180] *See* Scott Likens, *How Artificial Intelligence Is Already Disrupting Financial Services*, Barrons (May 16, 2019), *available at* https://www.barrons.com/articles/how-artificial-intelligence-is-already-disrupting-financial-services-51558008001.

[181] H.R. 4476, 116th Congress (U.S. House of Representatives).

[182] *Id.* (including the Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Deposit Insurance Corp., Federal Reserve, Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the National Credit Union Association and the Federal Housing Finance Agency).

[183] *Id.*

[184] Robert Booth, *Unilever saves on recruiters by using AI to assess job interviews*, The Guardian (Oct. 25, 2019), *available at* https://www.theguardian.com/technology/2019/oct/25/unilever-saves-on-recruiters-by-using-ai-to-assess-job-interviews; Lloyd Chinn & Thomas Fiascone, *AI In Hiring: Legislative Responses And Litigation Potential*, Law360 (Nov. 25, 2019), *available at* https://www.law360.com/illinois/articles/1220318/ai-in-hiring-legislative-responses-and-litigation-potential.

[185] H.R. 827 – AI JOBS Act of 2019, 116th Cong (2019), available at https://www.congress.gov/bill/116thcongress/house-bill/827/text.

[186] S. 2468, 116th Congress (U.S. Senate).

[187] *Id.*

[188] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Wash. Post (Oct. 25, 2019*), available at* https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[189] H.B. 2557, 2019-2020 Reg. Sess. (Ill. 2019) (101st Gen. Assembly), *available at* http://www.ilga.gov/legislation/101/HB/PDF/10100HB2557lv.pdf.

[190] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Wash. Post (Oct. 25, 2019), *available at* https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[191] For example, Washington State introduced legislation on January 23, 2019 that provides a private right of action and seeks to address the elimination of algorithmic bias through a careful consideration of fairness, accountability, and transparency. *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/. Under this law, an agency would be prohibited from using an automated decision-making system to discriminate against an individual on the basis of a list of factors such as race, national origin, sex, and age. *Id.*

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Frances Waldmann, Tony Bedel, Selina Grün, Emily Lamm and Chris Timura.

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, any member of the firm's Artificial Intelligence and Automated Systems Group, or the following authors:

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

Please also feel free to contact any of the following practice group members:

Artificial Intelligence and Automated Systems Group:

H. Mark Lyon - Chair, Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
J. Alan Bannister - New York (+1 212-351-2310, abannister@gibsondunn.com)
David H. Kennedy - Palo Alto (+1 650-849-5304, dkennedy@gibsondunn.com)
Ari Lanin - Los Angeles (+1 310-552-8581, alanin@gibsondunn.com)
Robson Lee - Singapore (+65 6507 3684, rlee@gibsondunn.com)
Carrie M. LeRoy - Palo Alto (+1 650-849-5337, cleroy@gibsondunn.com)

Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33 180, mwalther@gibsondunn.com)