GIBSON DUNN

Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems

Client Alert | January 29, 2021

In 2020, companies and regulators faced unprecedented challenges as they navigated the COVID-19 crisis and a rapidly evolving set of issues and policy proposals on the regulation of Artificial Intelligence and Automated Systems ("AI"). After a slow start, the second half of 2020 saw a noticeable surge in AI-related regulatory and policy proposals as well as growing international coordination. We may be seeing an inflection point in AI governance,[1] and 2021 is poised to bring consequential legislative and policy changes.

In the U.S., the fourth quarter 2020 saw federal rulemaking gather real pace. At the very end of 2020, Congress passed landmark legislation, the National Defense Authorization Act ("NDAA"), boosting the nascent U.S. national AI strategy, increasing spending for AI research funding, and raising the profile of the U.S. National Institute of Standards and Technology ("NIST") as the need for more coordination with respect to technical standards emerges as a policy priority. The expansion of AI research funding and coordination by the new National AI Initiative Office places the federal government in a more prominent role in AI research. Amid waning public trust in the use of tools for automated decision-making, 2020 also saw a number of federal bills promoting the ethical and equitable use of AI technologies and consumer protection measures.

The European Union ("EU") has emerged as a pacesetter in AI regulation, taking significant steps towards a long-awaited comprehensive and coordinated regulation of AI at EU level—evidence of the European Commission's (the "Commission") ambition to exploit the potential of the EU's internal market and position itself as a major player in sustainable technological innovation. This legislation is expected imminently, and all signs point to a sweeping regulatory regime with a system for AI oversight of high-risk applications that could significantly impact technology companies active in the EU.

Our 2020 Artificial Intelligence and Automated Systems Annual Legal Review examines a number of the most significant developments affecting companies as they navigate the evolving AI landscape, focusing on developments within the United States. We also touch, albeit non-exhaustively, on developments within the EU and the UK that may be of interest to domestic and international companies alike.

Related People

Frances Waldmann

Tony Bedel

Table of Contents

I. INTERNATIONAL POLICY DEVELOPMENTS

2020 saw a number of international initiatives looking to provide guidance and build a global consensus on the development and regulation of AI, including the OECD member states' recent adoption of OECD Principles on AI—the first international AI standards—and the establishment of the Global Partnership on Artificial Intelligence ("GPAI") in June 2020. We anticipate further international activity in 2021, including the Commission's forthcoming legislative proposals (*see* III. below).

A. Global Partnership on AI

In May 2019, Canada and France announced plans for a new international body for the G7 countries to study and steer the effects of AI on the world's people and economies by creating best practices, modeled on the UN's Intergovernmental Panel on Climate Change.[2] After previously expressing reluctance due to fears that the initiative's recommendations would harm innovation, on May 28, 2020, the U.S. Department of State announced that the United States had joined the GPAI—becoming the last of the G7 countries to sign on. On June 15, 2020, the UK Government issued a joint statement announcing the creation of the GPAI along with 14 other founding members, including the EU and the United States.[3] In the joint statement, GPAI is described as an "international and multistakeholder initiative to guide the responsible development and use of AI, grounded in human rights, inclusion, diversity, innovation, and economic growth." The initiative plans to support research and the "responsible and human-centric development and use of AI" by reference to the OECD Recommendation on AI.[4] GPAI's short term priority, however, is to investigate how AI can be used to help with the response to, and recovery from, COVID-19.

B. UK-U.S. Partnership on AI

On September 25, 2020, the UK and U.S. signed a "Declaration on Cooperation in Artificial Intelligence Research and Development," intended to promote a "shared vision" for AI in the areas of "economic growth, health and wellbeing, the protection of democratic values, and national security." The new partnership envisages that the UK and U.S.

governments will collaborate by (i) using bilateral science and technology cooperation and multilateral cooperation frameworks; (ii) recommending priorities for future cooperation, particularly in research and development (R&D) areas; (iii) coordinating the planning and programming of relevant activities in areas that have been identified; and (iv) promoting R&D in AI, focusing on challenging technical issues.

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

In February 2019, President Trump issued an Executive Order "Maintaining American Leadership in Artificial Intelligence," which marked the launch of the "American AI Initiative" and sought to accelerate AI development and regulation to secure the United States' place as a global leader in AI technologies.

Almost two years later, we have seen a significant increase in AI-related legislative and policy measures in the U.S. In particular, the federal government has been active in coordinating cross-agency leadership and encouraging the continued research and development of AI technologies for government use. To that end, a number of key legislative and executive actions focused on the growth and development of such technologies for federal agency, national security and military uses.

A. Policy Developments

1. Bipartisan U.S. Lawmakers Introduce Legislation to Create a National AI Strategy

On September 16, 2020, Reps. Robin Kelly (D-Ill.) and Will Hurd (R-Texas), after coordination with experts and the Bipartisan Policy Center, introduced a concurrent resolution calling for the creation of a national AI strategy.[5] This Resolution proposes four pillars to guide the strategy:[6]

- **Workforce**: Fill the AI talent gap and prepare American workers for the jobs of the future, while also prioritizing inclusivity and equal opportunity;[7]
- **National Security**: Prioritize the development and adoption of AI technologies across the defense and intelligence apparatus;
- **Research and Development**: Encourage the federal government to collaborate with the private sector and academia to ensure America's innovation ecosystem leads the world in AI; and
- **Ethics**: Develop and use AI technology in a way that is ethical, reduces bias, promotes fairness, and protects privacy.

2. OMB Guidance for Federal Regulatory Agencies

In January 2020, the Office of Management and Budget ("OMB") published a draft memorandum featuring 10 "AI Principles"[8] and outlining its proposed approach to regulatory guidance for the private sector which echoes the "light-touch" regulatory approach espoused by the 2019 Executive Order, 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."[9] As expected, the principles favored flexible regulatory frameworks consistent with the Executive Order[10] 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.

On November 17, 2020, the OMB issued its final guidance to federal agencies on when and how to regulate the private sector use of AI, presenting a broad perspective on AI oversight generally in keeping with its flexible, anti-regulatory approach eschewing "precautionary regulation" or "[r]igid, design-based regulations."[11] The OMB guidance urges agencies to first assess the effects in order to avoid "regulatory and non-regulatory actions that needlessly hamper AI innovation and growth," and provides technical guidance on rule-making, including a "regulatory impact assessment."[12] The OMB then prompts immediate action by requiring federal agencies to provide compliance plans, which will then be made public via each agency's website, by May 17, 2021. These plans should document the agency's regulatory authorities over "high-priority AI applications," collections of "AI-related information" from regulated entities (and any restrictions on the collection or sharing of such information), the outcomes of stakeholder engagements that identify existing regulatory barriers to AI applications within that agency's purview, and any planned regulatory actions.[13] The OMB guidance also repeats its previous comments on the need "to address inconsistent, burdensome, and duplicative State laws" that might prevent the emergence of a national market, but to avoid regulatory action in instances where a uniform national standard is not essential.[14]

3. Executive Order on Federal Agency Use of AI

On December 3, 2020, President Trump signed a second Executive Order ("EO") on AI, providing guidance for federal agency adoption of AI for government decision-making in a manner that protects privacy and civil rights. Numerous government agencies already use AI systems as predictive enforcement tools and to process and review vast amounts of data to detect trends and shape policymaking.[15]

The EO set out nine principles for the design, development, acquisition and use of AI in government in an effort "to foster public trust and confidence in the use of AI, and ensure that the use of AI protects privacy, civil rights, and civil liberties." The order emphasizes AI use must be "lawful; purposeful and performance-driven; accurate, reliable, and effective; safe, secure, and resilient; understandable; responsible and traceable; regularly monitored; transparent; and accountable."

The EO directs agencies to prepare inventories of AI-use cases throughout their departments (excluding classified or sensitive use cases) by July 2021, which could provide new insights into how federal agencies currently deploy AI technology. Emphasizing that ongoing adoption, deployment and acceptance of AI will depend significantly on public trust, the EO tasks the OMB with charting a roadmap for policy guidance by May 2021 for how agencies should use AI technologies in all areas excluding national security and defense.

B. NIST Report on the Four Principles of Explainable Artificial Intelligence

In February 2019, the Trump administration's Executive Order on Maintaining American Leadership in Artificial Intelligence directed NIST to develop a plan that would, among other objectives, "ensure that technical standards minimize vulnerability to attacks from malicious actors and reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies; and develop international standards to promote and protect those priorities." In response, NIST issued a plan in August 2019 for prioritizing federal agency engagement in the development of AI standards, identifying seven properties that characterize trustworthy AI—accuracy, explainability, resiliency, safety, reliability, objectivity, and security.[16]

In August 2020, NIST published a white paper on the Four Principles of Explainable Artificial Intelligence that "comprise the fundamental properties for explainable AI systems."[17] The four principles for explainable AI are:

- **Explanation**: AI systems should deliver accompanying evidence or reasons for all their outputs.
- **Meaningful**: Systems should provide explanations that are meaningful or understandable to individual users.
- **Explanation Accuracy**: The explanation correctly reflects the system's process for generating the output.
- **Knowledge Limits**: The system only operates under conditions for which it was designed or when the system reaches a sufficient confidence in its output.

According to NIST, evaluating explainability in context of human decision-making also may lead to better understanding of human–machine collaboration and interfaces. Since humans demonstrate only a limited ability to meet the four principles described above, NIST discusses that human decision-making may provide a benchmark to evaluate explainable AI systems and informs the development of reasonable metrics. The public comment period closed on October 15, 2020.

C. Legislative Developments

In the first half of 2020, the effect of the unprecedented COVID-19 pandemic stalled much of the promised legislative progress, and many of the ambitious bills intended to build a regulatory framework for AI languished in committee and have not been passed. But, despite political gridlock, AI-related federal legislation continued to draw bipartisan Congressional enthusiasm in 2020, and at the end of the year, Congress passed—in dramatic fashion—the most significant and wide-ranging AI-related legislation to date. Bills pending before the last Congress that did not pass a floor vote will need to be reintroduced in the new Congress that was sworn in on January 3.

1. National Defense Authorization Act, H.R. 6395

On January 1, 2021, the 116th Congress overrode a presidential veto and passed the Fiscal Year 2021 National Defense Authorization Act ("NDAA")—a $731.6 billion defense bill—into law.[18] The NDAA represents a significant step forward for AI policy in the U.S. far beyond national defense, and establishes a regulatory framework for coordinating AI research and policy across the federal government, as well as a national network of AI research institutes focusing on mission-driven research to be led by the National Science Foundation ("NSF), the Department of Energy ("DoE"), the Department of Commerce, NASA and the Department of Defense ("DoD"). The NDAA is likely to influence AI policy across the regulatory spectrum—from private sector development, testing, and deployment of AI systems, to mandatory federal guidelines, technical standards and voluntary risk management frameworks.

The legislation includes both DoD and non-DoD AI provisions and draws on legislation introduced earlier this year, the National Artificial Intelligence Initiative Act of 2020 (H.R. 6216), as well as the 2019 Artificial Intelligence Initiative Act (S. 1558), to establish a coordinated federal initiative to accelerate research and development and encourage investments in trustworthy AI systems.[19] The NDAA also includes select provisions from a number of other draft bills introduced in 2020, including four bills introduced by the nascent bipartisan Senate AI Caucus.[20]

Of particular note are measures to create a new "National Artificial Intelligence Initiative Office" to be led by the White House, to order the Pentagon to take steps to ensure the AI technologies it acquires are developed in an ethically and responsibly sourced manner,

and to charge NIST with developing an "AI Risk Management Framework." The NDAA also includes a provision to make computational resources and robust data sets publicly available for researchers across the country through a "National Research Cloud."[21] The bill authorizes nearly $5 billion in funding for AI research at NSF over the next five years ($4.796 billion), $1.15 billion at the DoE, and $390 million at NIST. The NDAA affords industry stakeholders a number of opportunities to shape federal agencies' use of AI systems as well as to participate in discussions surrounding best practices and technical standards.

a) Department of Defense AI Provisions

The NDAA directs the Secretary of Defense to assess, within 180 days of passage, whether the DoD has the ability, requisite resourcing, and sufficient expertise to ensure that any AI technology acquired by DoD is ethically and responsibly developed, and must provide a briefing of the assessment's results to Congress within 30 days of its completion.[22]

The NDAA also assigns responsibility for DoD's Joint Artificial Intelligence Center ("JAIC") to the Deputy Secretary of Defense to "ensure data access and visibility for the JAIC." Moreover, the NDAA grants the JAIC Director acquisition authority in support of defense missions of up to $75 million for new contracts for each year through FY2025.

b) Non-Department of Defense AI Provisions

The NDAA includes a measure for the creation of a new **National AI Initiative Office** to be established by the Director of the White House Office of Science and Technology Policy ("OSTP") to lead U.S. global leadership in the development and use of trustworthy AI systems and prepare the nation's workforce for the integration of AI across all sectors of the economy.[23] The office's mission is to serve as the point of contact for federal AI activities for federal departments and agencies, as well as other public and private entities.

The initiative will functionally consist of two organizations. First, the **Interagency Committee** will be tasked with providing coordination of federal AI research and development activities as well as education and workforce training activities across the government.[24] Within two years of the passage of the NDAA, the Committee is to develop a strategic plan that establishes goals, priorities, and metrics for guiding and evaluating how federal agencies will "prioritize areas of AI research and development, examines long-term funding for interdisciplinary AI research, and supports research on ethical, legal, environmental, safety, security, bias, and other issues related to AI and society."[25] The companion body to the Interagency Committee is a new external **National AI Advisory Committee** to be established by the Secretary of Commerce in consultation with Director of OSTP, the Attorney General, the Director of National Intelligence, and the Secretaries of Defense, Energy, and State.[26] The Advisory Committee will then create a subcommittee on AI and law enforcement to advise the White House on bias (including the use of facial recognition by government authorities), data security, adoptability, and legal standards (including those designed to ensure the use of AI systems are consistent with the privacy rights, civil rights and civil liberties, and disability rights issues raised by the use of these technologies.)[27]

The Director of the NSF, in coordination with OSTP, is tasked with establishing a **National AI Research Task Force** to investigate the feasibility of establishing and sustaining a National AI Research Resource and to propose a roadmap and implementation plan detailing how such a resource should be established and sustained.[28] The Director of the NSF is also permitted to establish a network of **National AI Research Institutes** that are focused on cross-cutting challenges for AI systems, like trustworthiness or foundational science, or those that are focused on a particular economic or social sector such as health care, education, manufacturing.[29] These institutes are to include a component addressing the ethical and safety implications of the relevant application of AI

to that sector and are to be funded for a renewable period of five years.

While **NIST** has already been active on AI issues, particularly with respect to standard-setting and trust-worthy AI, the NDAA further increases NIST's AI responsibilities through a legislative mandate on AI, expanding its mission to include advancing collaborative frameworks, standards, guidelines for AI, supporting the development of a risk-mitigation framework for AI systems, and supporting the development of technical standards and guidelines to promote trustworthy AI systems.[30] In addition to developing best practices and voluntary standards for privacy and security in training datasets, computer chips/hardware, and data management techniques, NIST will be responsible for developing, within two years, a **Risk Management Framework** that "identifies and provides standards for assessing the trustworthiness of AI systems, establishes common definitions for common terms such as explainability, transparency, safety, and privacy, provides case studies of successful framework implementation, and aligns with international standards no later than two years after the passage of the NDAA."[31]

2. Securing American Leadership in Science and Technology Act of 2020

On January 28, 2020, Representative Frank Lucas (R-OK) and 12 Republican cosponsors, introduced the Securing American Leadership in Science and Technology Act of 2020 ("SALTA"), (H.R. 5685), a bill broadly focused on "invest[ing] in basic scientific research and support technology innovation for the economic and national security of the United States."[32]

The bill would have the NIST promote U.S. "innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve Americans' quality of life."

3. Generating Artificial Intelligence Networking Security ("GAINS") Act

May 2020 saw the introduction of the Generating Artificial Intelligence Networking Security ("GAINS") Act (H.R. 6950), which directs the Department of Commerce and the Federal Trade Commission to identify the benefits and barriers to AI adoption in the U.S., survey other nations' AI strategies and rank how the U.S. compares; and assess the supply chain risks and how to address them.[33] The bill, which was referred to the Committee on Energy and Commerce but did not advance, requires the agencies to report the results to Congress, along with recommendations to develop a national AI strategy.

4. The AI in Government Act of 2020

The AI in Government Act of 2020 (H.R. 2575) was passed by the House on September 14, 2020 by voice vote.[34] The bill aims to promote the efforts of the federal government in developing innovative uses of AI by establishing the "AI Center of Excellence" within the General Services Administration ("GSA"), and requiring that the OMB issue a memorandum to federal agencies regarding AI governance approaches. It also requires the OSTP to issue guidance to federal agencies on AI acquisition and best practices. An identical bill, S. 1363, which was approved by the U.S. Senate Homeland Security and Governmental Affairs Committee in November 2019, has not passed.[35]

III. EU POLICY &

REGULATORY DEVELOPMENTS

In past years, EU discussions about regulating AI technologies had been characterized by a restrictive "regulate first" approach.[36] However, the regulatory road map presented by the Commission in February 2020 under the auspices of its new digital strategy eschewed, for example, blanket technology bans and proposed a more nuanced "risk-based" approach to regulation, emphasizing the importance of "trustworthy" AI but also acknowledging the need for Europe to both remain innovative and competitive in a rapidly growing space and avoid fragmentation of the single market resulting from differences in national legislation.

The Commission's "White Paper on Artificial Intelligence – A European approach to excellence and trust" (the "White Paper") sets out a road map designed to balance innovation, ethical standards and transparency.[37] As noted in our legal update "EU Proposal on Artificial Intelligence Regulation Released," the White Paper favors a risk-based approach with sector- and application-specific risk assessments and requirements, rather than blanket sectoral requirements or bans—earmarking a series of "high-risk" technologies for future oversight, including those in "critical sectors" and those deemed to be of "critical use."[38] The Commission also released a series of accompanying documents: the "European Strategy for Data" ("Data Strategy")[39] and a "Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics" ("Report on Safety and Liability").[40]

Although the Commission is seeking to impose a comprehensive and harmonious framework for AI regulation across all member states, there is no clear consensus as to the scope of regulatory intervention. In October 2020, 14 EU members (Denmark, Belgium, the Czech Republic, Finland, France, Estonia, Ireland, Latvia, Luxembourg, the Netherlands, Poland, Portugal, Spain and Sweden) published a joint position paper urging the Commission to espouse a "soft law approach" that takes into account the fast-evolving nature of AI technologies and favors self-regulation and voluntary practices to avoid harming innovation.[41] Germany, on the other hand, has expressed concern over certain Commission proposals to apply restrictions on AI applications deemed to be of high-risk only, and favors a broader regulatory reach for technologies that would be subject to the new framework, as well as mandatory, detailed rules for data retention, biometric remote identification and human supervision of AI systems.[42]

In short, while the Commission's comprehensive legislative proposal is expected imminently, the EU policy landscape has remained dynamic in the lead up. Companies active in AI should closely follow recent developments in the EU, given the proposed geographic reach of the future AI legislation, which is likely to affect all companies doing business in the EU.

A. European Commission's AI White Paper Consultation and "Inception Impact Assessment"

As we reported in our Artificial Intelligence and Automated Systems Legal Update (1Q20), in January 2020, the EC launched a public consultation period and requested comments on the proposals set out in the White Paper and the Data Strategy, providing an opportunity for companies and other stakeholders to provide feedback and shape the future EU regulatory landscape. In July, the Commission published a summary report on the consultation's preliminary findings.[43] Respondents raised concerns about the potential for AI to breach fundamental rights or lead to discriminatory outcomes, but they

were divided on whether new compulsory requirements should be limited to high-risk applications.

On the heels of the White Paper Consultation, the Commission launched an "Inception Impact Assessment" initiative for AI legislation in July 2020, aiming to define the Commission's scope and goals for AI legislation with a focus on ensuring that "AI is safe, lawful and in line with EU fundamental rights."[44] The Commission's road map builds on the proposals in the White Paper and provides more detail on relevant policy options and policy instruments, from a "baseline" policy (involving no policy change at the EU level) through various alternative options following a "gradual intervention logic," ranging from a non-legislative, industry-led, "soft law" approach (Option 1) through a voluntary labelling scheme (Option 2), to comprehensive and mandatory EU-level legislation for all or certain types of AI applications (Option 3), or a combination of any of the options above taking into account the different levels of risk that could be generated by a particular AI application (Option 4).[45] Another core question relates to the scope of the initiative, notably how AI should be defined (narrowly or broadly) (e.g., machine learning, deep neural networks, symbolic reasoning, expert systems, automated decision-making).

Substantively, the road map reiterates that the Commission is particularly concerned with a number of specific, significant AI risks that are not adequately covered by existing EU legislation, such as cybersecurity, the protection of employees, unlawful discrimination or bias, the protection of EU fundamental rights, including risks to privacy, and protecting consumers from harm caused by AI (both through existing and new product safety legislation). Continued focus remains on the need for legal certainty, both for business marketing products involving AI in the EU, and for market surveillance and supervisory authorities. The feedback period for the road map closed in September, and the completion of the Inception Impact Assessment was scheduled for December 2020. As noted, these policy proposals are intended to culminate in proposed regulation, which is expected to be unveiled by the Commission in the first quarter of 2021.

B. European Parliament Votes on Proposals regarding the Regulation of Artificial Intelligence

Earlier this year, the European Parliament set up a special committee to analyze the impact of artificial intelligence on the EU economy[46] to ensure that the EU "develops AI that is trustworthy, eliminates biases and discrimination, and serves the common good, while ensuring business and industry thrive and generate economic prosperity."[47]

In April 2020, the Parliament's Legal Affairs Committee ("JURI") published three draft reports to the Commission providing recommendations on a framework for AI liability, copyright protection for AI-assisted human creations, safeguards within the EU's patent system to protect the innovation of AI developers, and AI ethics and "human-centric AI."[48] The three legal initiatives, summarized in final reports and recommendations outlined in more detail below, were adopted by the plenary on October 20, 2020.[49]

1. Report with Recommendations to the Commission on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies

The legislative initiative urges the Commission to present a legal framework outlining the ethical principles and legal obligations to be followed when developing, deploying and using artificial intelligence, robotics and related technologies in the EU including software, algorithms and data, protection for fundamental rights. The initiative also calls for the establishment of a "European Agency for Artificial Intelligence" and a "European certification of ethical compliance."[50]

The proposed legal framework is premised on several guiding principles, including

"human-centric and human-made AI; safety, transparency and accountability; safeguards against bias and discrimination; right to redress; social and environmental responsibility; and respect for privacy and data protection."[51] High-risk AI technologies, which include machine learning and other systems with the capacity for self-learning, should be designed to "allow for human oversight and intervention at any time, particularly where a functionality could result in a serious breach of ethical principles and could be dangerous."[52] Some of the high-risk sectors identified are healthcare, public sector and finance, banking and insurance.

2. Report with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence

The Report calls for a future-oriented civil liability framework that makes front- and back-end operators of high-risk AI strictly liable for any resulting damage and provides a "clear legal framework [that] would stimulate innovation by providing businesses with legal certainty, whilst protecting citizens and promoting their trust in AI technologies by deterring activities that might be dangerous."[53] While it does not take the position that a new EU liability regime is necessary, the Report identifies a gap in the existing EU product liability regime with respect to the liability of operators of AI-systems in the absence of a contractual relationship with potential victims, proposing a dual approach: (1) strict liability for operators of "high-risk AI-systems" akin to the owner of a car or pet; or (2) a presumption of fault towards the operator for harm suffered by a victim by a non-"high-risk" AI system, with national law regulating the amount and extent of compensation as well as the limitation period in case of harm caused by the AI-system.[54] Multiple operators would be held jointly and severally liable, subject to a maximum liability of €2 million. The Report defines criteria on which AI-systems can qualify as high-risk in the Annex, proposing that a newly formed standing committee, involving national experts and stakeholders, should support the Commission in its review of potentially high-risk AI-systems.

3. Report on Intellectual Property Rights for the Development of Artificial Intelligence Technologies

The Report emphasizes that EU global leadership in AI requires an effective intellectual property rights system and safeguards for the EU's patent system in order to protect and incentivize innovative developers, balanced with the EU's ethical principles for AI and consumer safety.[55] Notably, the Report distinguishes between AI-assisted human creations and AI-generated creations, taking the position that AI should not have a legal personality and that ownership of IP rights should only be granted to humans. Where AI is used only as a tool to assist an author in the process of creation, the current intellectual property legal framework should remain applicable. Nonetheless, the Report recommends that AI-generated creations should fall under the scope of the EU intellectual property regime in order to encourage investment and innovation, subject to protection under a specific form of copyright.

C. European Commission's Assessment List for Trustworthy AI

As we noted in our 2019 Artificial Intelligence and Automated Systems Annual Legal Review, 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").[56]

On July 17, 2020, the AI HLEG presented its final "Assessment List for Trustworthy AI," a tool intended to help companies "self-assess" and identify the risks of AI systems they develop, deploy or procure, and implement the Ethics Guidelines in order to mitigate those risks.[57] A previous version of the Assessment List was included in the April 2019 Ethics Guidelines, and this final Assessment List represents an amended version following a

piloting process in which over 350 stakeholders participated. The Assessment List is designed as a flexible framework that companies can adapt to their particular needs and the sector they operate in order to minimize specific risks an AI system might generate. The Assessment List proposes a tailored series of self-assessment questions for each of the seven principles for trustworthy AI set out in the AI HLEG's Ethics Guidelines (Human Agency and Oversight; Technical Robustness and Safety; Privacy and Data Governance; Transparency; Diversity, Non-Discrimination and Fairness; Societal and Environmental Well-being; and Accountability). The AI HLEG recommends that the tool be used by a "multidisciplinary team."

D. Council of Europe Publishes Feasibility Study on Developing a Legal Instrument for Ethical AI

On December 17, 2020, the Council of Europe's Ad hoc Committee on Artificial Intelligence ("CAHAI") published a report examining both the feasibility and possible constituent elements of a legal framework for the development and application of AI systems, based on "the Council of Europe's standards in the field of human rights, democracy and the rule of law."[58] The report identifies nine principles that are essential to respect human rights in the context of AI: Human Dignity; Prevention of Harm to Human Rights, Democracy, and the Rule of Law; Human Freedom and Human Autonomy; Non-Discrimination, Gender Equality, Fairness and Diversity; Principle of Transparency and Explainability of AI Systems; Data Protection and the Right to Privacy; Accountability and Responsibility; Democracy; and the Rule of Law.

The report concludes that current international and national regulations do not sufficiently address the challenges posed by AI, and proposes the development of a new legal framework for AI consisting of both binding (such as model national legislation) and nonbinding Council of Europe instruments. Much like the AI HLEG's Ethics Guidelines for Trustworthy AI and the European Commission's White Paper on AI, the Council of Europe's study proposes a risk-based approach to regulating AI—acknowledging that not all AI systems pose an equally high level of risk—and seeks to balance legal certainty for AI stakeholders while providing broad regulatory guidance to companies implementing governance regimes. The study will be presented to the Committee of Ministers of the Council of Europe, who may instruct CAHAI to begin developing the specific elements of a legal framework for AI.

E. German Inquiry Committee Report on Artificial Intelligence

In November 2020, the German AI inquiry committee (Enquete-Kommission Künstliche Intelligenz des Deutschen Bundestages, "Committee") presented its final report, which provides broad recommendations on how society can benefit from the opportunities inherent in AI technologies while acknowledging the risks they pose.[59]

The Committee's work placed a focus on legal and ethical aspects of AI and its impact on the economy, public administration, cybersecurity, health, work, mobility, and the media. The Committee advocates for a "human-centric" approach to AI, a harmonious Europe-wide strategy, a focus on interdisciplinary dialog in policy-making, setting technical standards, legal clarity on testing of products and research, and the adequacy of digital infrastructure.

At a high level, the Committee's specific recommendations relate to (1) data-sharing and data standards; (2) support and funding for research and development; (3) a focus on "sustainable" and efficient use of AI; (4) incentives for the technology sector and industry to improve scalability of projects and innovation; (5) education and diversity; (6) the impact of AI on society, including the media, mobility, politics, discrimination and bias; and (7) regulation, liability and trustworthy AI.

IV. UK POLICY & REGULATORY DEVELOPMENTS

In the past several years, the UK has focused on developing a national position on a number of specific AI-related issues, such as data protection, explainability, and autonomous vehicles, but otherwise has not enacted any laws or regulations that govern the use of AI technologies. As its national strategy on AI continues to take shape, the UK may soon find itself at a regulatory crossroads. While UK companies selling AI-related products or services into the EU would likely have to comply with the new European regime, the House of Lords Select Committee on AI—which was appointed in June 2017 to "consider the economic, ethical and social implications of advances" in AI—has generally indicated a reluctance to establish a cross-cutting regulatory framework for AI in favor of sector-specific regulation.

In February 2020, the UK Government's Committee on Standards in Public Life published a report on "Artificial Intelligence and Public Standards," addressing the deployment of AI in the public sector.[60] Although it also did not favor the creation of a specific AI regulator, it described the new Centre for Data Ethics and Innovation ("CDEI") as a "regulatory assurance" body with a cross-cutting role, and went on to identify an urgent need for guidance and regulation on the issues of transparency and data bias, in particular. In June 2020, CDEI published its "AI Barometer," a risk-based analysis which reviews five key sectors (criminal justice, health and social care, financial services, energy and utilities and digital and social media) and identifies opportunities, risks, barriers and potential regulatory gaps.[61] The UK also participated in the drafting of the Council of Europe's Feasibility Study on Developing a Legal Instrument for Ethical AI (see III.D. above).

A. AI Council National AI Strategy

In January 2021, the AI Council, an independent expert and industry committee that advises the UK Government on artificial intelligence, published an "AI Roadmap," recommending the deployment of a national UK AI strategy.[62] The AI Council's 16 recommendations identify and address challenges to the advancement across a number of sectors: research, development and innovation; skills & diversity; data, infrastructure & public trust; and national, cross-sector adoption. The roadmap advises that the UK should lead in developing appropriate standards to frame the future governance of data and enact "clear and flexible regulation" building on existing guidance from regulators such as the Information Commissioner's Office ("ICO").

The AI Council also focuses on public trust and algorithmic accountability, noting that "the public should be reassured that the use of AI is safe, secure, fair, ethical and overseen by independent entities." In addition to continuous development of industry standards and suitable regulations and frameworks for algorithmic accountability, it does not rule out the need for further legislation, such as a public interest data bill to ensure transparency about automated decision-making, the right for the public to give meaningful input (for example, through algorithmic impact assessments), and the ability for regulators to enforce sanctions.[63]

B. House of Lords' Liaison Committee Report: "AI in the UK: No Room for Complacency"

In December 2020, the House of Lords' Liaison Committee ("Committee") published a report "AI in the UK: No Room for Complacency" (the "2020 Report"), a follow up on the 2018 Report by the House of Lords' Select Committee (the "2018 Report").[64]

The 2018 Report emphasized that blanket AI-specific regulation is not appropriate and existing sector-specific regulators are best placed to consider the impact on their sectors of any subsequent regulation which may be needed. It also noted that GDPR addressed many of the concerns with respect to AI and data, and tasked the CDEI with identifying any gaps in existing regulation.

The 2020 Report continued to espouse a regulator-led approach, noting that individual industry sectors are best placed to identify the regulation needed in their area, and proposing that industry stakeholders should take the lead in establishing voluntary mechanisms for informing the public when artificial intelligence is being used for significant or sensitive decisions in relation to consumers, tasking the AI Council with the development and implementation of these mechanisms. However, as previewed, the 2020 Report also raised concerns about deficiencies in the existing legal framework for certain AI use cases, such as facial recognition technology, and flags that a solely self-regulatory approach to ethical standards risks a lack of uniformity and enforceability as well as a lack of public trust in the use of AI.

Moreover, the 2020 Report recommended that, by July 2021, and with input from CDEI, Office for AI and Alan Turing Institute, the ICO should develop and roll out a training course for use by regulators to ensure they have a grounding in the ethical and appropriate use of public data and AI systems, and its opportunities and risks. CDEI is also tasked with establishing and publishing international standards for the ethical development of AI, including issues of bias, and for the ethical use of AI by policymakers and businesses.

C. UK ICO Guidance on AI and Data Protection

On July 30, 2020, the ICO published its final guidance on Artificial Intelligence (the "Guidance").[65] Intended to help organizations "mitigate the risks of AI arising from a data protection perspective without losing sight of the benefits such projects can deliver," the Guidance sets out a framework and methodology for auditing AI systems and best practices for compliance with the UK Data Protection Act 2018 and data protection obligations under the EU's General Data Protection Regulation ("GDPR"). The Guidance proposes a "proportionate and risk-based approach" and recommends an auditing methodology consisting of three key parts: auditing tools and procedures for use in audits and investigations; detailed guidance on AI and data protection; and a tool kit designed to provide further practical support to organizations auditing the compliance of their own AI systems. The guidance addresses four overarching principles:

Accountability and governance in AI—including data protection impact assessments ("DPIAs"), understanding the relationship and distinction between controllers and processors in the AI context, as well as managing, and documenting decisions taken with respect to competing interests between different AI-related risks (e.g., trade-offs);

Fair, lawful and transparent processing—including how to identify lawful bases (and using separate legal bases for processing personal data at each stage of the AI development and deployment process), assessing and improving AI system performance, mitigating potential discrimination, and documenting the source of input data as well as any inaccurate input data or statistical flaw that might impact the output of the AI system.

Data minimization and security—including guidance to technical specialists on data security issues common to AI, types of privacy attacks to which AI systems are susceptible, compliance with the principle of data minimization (the principle of identifying the minimum amount of personal data needed, and to process no more than that amount

of information), and privacy-enhancing techniques that balance the privacy of individuals and the utility of a machine learning system during the training and inference stages.[66]

Compliance with individual data subject rights—including data subject rights in the context of data input and output of AI systems, rights related to automated decision, and requirements to design AI systems to facilitate effective human review and critical assessment and understanding of the outputs and limitations of AI systems.

The Guidance also emphasizes that data protection risks should be considered at an early stage in the design process (e.g., "safety by design") and that the roles of the different parties in the AI supply chain should be clearly mapped at the outset. Of note is also the recommendation that training data be stored at least until a model is established and unlikely to be retrained or modified. The Guidance refers to, but does not provide guidance on, the anonymization or pseudonymization of data as a privacy-preserving technique, but notes that the ICO is currently developing new guidance in this field.[67]

The ICO encouraged organizations to provide feedback on the Guidance to make sure that it remains "relevant and consistent with emerging developments."

V. REGULATION OF SPECIFIC AI TECHNOLOGIES AND USE CASES

A. Algorithmic Accountability and Consumer Safety

In 2020, a number of potential bills and policy measures addressing algorithmic accountability and transparency hinted at a shift amid growing public awareness of AI's potential to pose a risk to consumers, including by creating bias or harming certain groups.[68]

1. Consumer Safety Technology Act (H.R. 8128)

On September 29, 2020, the House passed the Consumer Safety Technology Act (H.R. 8128), previously named the "AI for Consumer Product Safety Act." If enacted, the bill would direct the U.S. Consumer Product Safety Commission ("CPSC") to establish a pilot program to explore the use of artificial intelligence for at least one of the following purposes: (1) tracking injury trends; (2) identifying consumer product hazards; (3) monitoring the retail marketplace for the sale of recalled consumer products; or (4) identifying unsafe imported consumer products. The bill has been referred to the Senate Committee on Commerce, Science, and Transportation.

2. Senators' Letter to EEOC Signals Scrutiny of AI Bias

On December 8, 2020, 10 U.S. senators sent a letter to the Chair of the U.S. Equal Employment Opportunity Commission ("EEOC"), urging the EEOC to use its powers under Title VII of the Civil Rights Act of 1964 to "investigate and/or enforce against discrimination related to the use of" AI hiring technologies.[69] The letter signals increased

enforcement and regulatory activity on the horizon for employment-related uses of technology in the hiring and employment process.

Lawmakers expressed particular concerns over “tools used in the employee selection process to manage and screen candidates after they apply for a job”; “new modes of assessment, such as gamified assessments or video interviews that use machine-learning models to evaluate candidates”; “general intelligence or personality tests”; and “modern applicant tracking systems.”

The lawmakers recognize that “hiring technologies can sometimes reduce the role of individual hiring managers’ biases,” but that “they can also reproduce and deepen systemic patterns of discrimination reflected in today’s workforce data.” The letter includes three specific questions: (1) can the EEOC request access to “hiring assessment tools, algorithms, and applicant data from employers or hiring assessment vendors and conduct tests to determine whether the assessment tools may produce disparate impacts?”; (2) if the EEOC were to conduct such a study, could it publish its findings in a public report?; and (3) what additional authority and resources would the EEOC need to proactively study and investigate these AI hiring assessment technologies?

3. A.B. 2269

A.B. 2269, “the Automated Decision Systems Accountability Act of 2020,” failed to progress through the California state legislature.[70] The bill would have required any business that uses an “automated decision system” (“ADS”) to “continually test for biases during the development and usage of the ADS, conduct an ADS impact assessment on its program or device to determine whether the ADS has a disproportionate adverse impact on a protected class….” ADS is defined broadly as “a 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 persons.” The bill had potentially significant consequences for a wide range of companies given that the definition of ADS, as it was defined, potentially implicated any computational process with an output that “impacts persons.”

B. Facial Recognition Software

1. Federal Regulation

Over the past several years, biometric surveillance, or “facial recognition technology,” emerged as a lightning rod for public debate regarding the risk of improper algorithmic bias and data privacy concerns, resulting in a string of efforts by various cities in the U.S.[71] to ban the use of facial recognition technology by law enforcement and some limited state legislation (California’s A.B. 1215).[72] During 2020, both federal, state governments indicated a willingness to enact regulations on the use of facial recognition technology by government agencies or law enforcement.

a) Ethical Use of Facial Recognition Act, S. 3284

On February 12, 2020, Senator Jeff Merkley (D-OR) introduced the Ethical Use of Facial Recognition Act, co-sponsored by Senator Cory Booker (D-NJ).[73] The bill would prohibit any federal officer, employee, or contractor from engaging in particular activities with respect to facial recognition technology without a warrant until a congressional commission recommends rules to govern the use and limitations of facial recognition technology for government and commercial uses. The prohibited activities include: setting up a camera to be used with facial recognition, accessing or using information obtain from facial recognition, or importing facial recognition to identify an individual in the U.S. Victims of violations of the bill would be permitted to bring a civil action for injunctive or declaratory relief in federal court. The bill would also prohibit state or local governments from investing

in, purchasing, or obtaining images from facial recognition technology.

b) Facial Recognition and Biometric Technology Moratorium Act of 2020

In June 2020, Democratic Senators and Representatives introduced the Facial Recognition and Biometric Technology Moratorium Act of 2020, which would impose limits on the use of biometric surveillance systems, such as facial recognition systems, by federal and state government entities. The bill also provided that any information obtained in violation of this bill would not be admissible by the federal government in any proceeding or investigation, except in a proceeding alleging a violation of this bill.

2. State and City Regulations

In 2020, several states passed, and others introduced, bills directly targeting facial biometrics.[74] In September 2020, the city of Portland, Oregon joined the list of cities that have enacted bans on certain uses of facial recognition technology.[75] Portland's law is the first in the U.S., however, to limit the use of facial recognition technology by the private sector. Subject to narrow exceptions,[76] the Ordinance prohibits its use by "private entities" in public places within the city, including stores, restaurants and hotels, taking effect on January 1, 2021.

a) Maryland, H.B. 1202

On May 8, 2020, Maryland enacted H.B. 1202, banning the use of "a facial recognition service for the purpose of creating a facial template during an applicant's interview for employment," unless the interviewee signs a waiver. The bill's definitions of the technology is directly aimed at AI: "'facial template' means the machine–interpretable pattern of facial features that is extracted from one or more images…."[77] The legislation appears to address a concern for potential hiring discrimination that may be borne out of these automated systems, akin to Illinois' Artificial Intelligence Video Interview Act (effective January 1, 2020), or "AI Video Act," which similarly required applicants to be notified and consent to the use of AI video analysis during interviews.[78]

b) Washington, S.B. 6280

In March 2020, Washington Governor Jay Inslee approved S.B. 6280, which would curb governmental use of facial recognition, prohibiting the use of such technology for ongoing surveillance and limits its use to acquiring evidence of serious criminal offences following authorization of a search warrant. The new law requires bias testing, training to safeguard against potential abuses, and disclosure when the state of Washington or its localities would employ facial recognition. Governor Inslee also partially vetoed the law, eliminating a provision which would establish a legislative task force that would provide recommendations regarding the potential abuses, safeguards, and efficacy of facial recognition services.[79] The law becomes effective on July 1, 2021.

C. Autonomous Vehicles

1. U.S. Federal Developments

a) DOT Acts on Updated Guidance for AV Industry

In January 2020, the Department of Transportation ("DoT") published updated guidance for the regulation of the autonomous vehicle ("AV") industry, "Ensuring American Leadership in Automated Vehicle Technologies" or "AV 4.0."[80] 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.[81] 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.

b) DOT Issues First-Ever Proposal to Modernize Occupant Protection Safety Standards for AVs

Shortly after announcing the AV 4.0, NHTSA in March 2020 issued its first-ever Notice of Proposed Rulemaking ("Notice") "to improve safety and update rules that no longer make sense such as requiring manual driving controls on autonomous vehicles."[82] The Notice aims to "help streamline manufacturers' certification processes, reduce certification costs and minimize the need for future NHTSA interpretation or exemption requests." For example, the proposed regulation would apply front passenger seat protection standards to the traditional driver's seat of an AV, rather than safety requirements that are specific to the driver's seat. Nothing in the Notice would make changes to existing occupant protection requirements for traditional vehicles with manual controls.[83]

c) SELF-DRIVE Act Reintroduced in U.S. Congress

Federal regulation of AVs had so far faltered in Congress, leaving the U.S. without a federal regulatory framework while the development of autonomous vehicle technology continues apace. However, on September 23, 2020, Rep. Bob Latta (R-OH) reintroduced the Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution ("SELF DRIVE") Act.[84] As we have addressed in previous legal updates,[85] the House previously passed the SELF DRIVE Act (H.R. 3388) 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)) stalled in the Senate.

The bill empowers the National Highway Traffic Safety Administration ("NHTSA") with the oversight of manufacturers of Highly Automated Vehicles ("HAVs") through enactment of future rules and regulations that will set the standards for safety and govern areas of privacy and cybersecurity relating to such vehicles. The bill also requires vehicle manufacturers to inform consumers of the capabilities and limitations of a vehicle's driving automation system and directs the Secretary of Transportation to issue updated or new motor vehicle safety standards relating to HAVs.

One key aspect of the bill is broad preemption of the states from enacting legislation that would conflict with the Act's provisions or the rules and regulations promulgated under the authority of the bill by the NHTSA. While state authorities would likely retain their ability to oversee areas involving human driver and autonomous vehicle operation, the bill contemplates that the NHTSA would oversee manufacturers of autonomous vehicles, just as it has with non-autonomous vehicles, to ensure overall safety. In addition, the NHTSA is required to create a Highly Automated Vehicle Advisory Council to study and report on the performance and progress of HAVs. This new council is to include members from a wide range of constituencies, including members of the industry, consumer advocates, researchers, and state and local authorities. The intention is to have a single body (the NHTSA) develop a consistent set of rules and regulations for manufacturers, rather than continuing to allow the states to adopt a web of potentially widely differing rules and regulations that may ultimately inhibit development and deployment of HAVs.

In a joint statement on the bill, Energy and Commerce Committee Republican Leader Rep. Greg Walden (R-OR) and Communications and Technology Subcommittee Republican

Leader Rep. Latta noted that "[t]here is a clear global race to AVs, and for the U.S. to win that race, Congress must act to create a national framework that provides developers certainty and a clear path to deployment."[86] The bill was referred to the House Energy and Commerce Committee and awaits further action. While it is expected that the new administration will push legislative action on AVs, it is not yet clear what the scope of such legislation may be.

d) NHTSA Launched New Automated Vehicle Initiative to Improve Safety, Testing, And Public Engagement

On June 15, 2020, NHTSA announced a new initiative to improve the safety and testing transparency of AVs, the Automated Vehicle Transparency and Engagement for Safe Testing ("AV TEST") Initiative.[87] The purpose of the AV TEST Initiative is to share information concerning the safe development and testing of AVs. In addition to "creating a formal platform for Federal, State, and local government to coordinate and share information in a standard way," the Department is also creating a public-facing platform where companies and governments can choose to share on-road testing locations and testing activity data, such as vehicle types and uses, dates, frequency, vehicle counts, and routes.[88]

Although the AV TEST Initiative may provide welcome centralization, some safety advocates are critical of the Department's voluntary approach and failure to develop minimum performance standards.[89]

e) NHTSA Released Report on Federal Motor Vehicle Safety Standards Considerations ("FMVSS") for AVS

In April 2020, NHTSA released research findings on twelve Federal Motor Vehicle Safety Standards Considerations ("FMVSS") related to vehicles with automated driving systems—six crash avoidance standards and six crashworthiness standards.[90] Specifically, the project evaluated options regarding technical translations of FMVSS, including the performance requirements and the test procedures, and related Office of Vehicle Safety Compliance ("OVSC") test procedures, that may impact regulatory compliance of vehicles equipped with automated driving systems. The report evaluated the regulatory text and test procedures with the goal of identifying possible options to remove regulatory barriers for the compliance verification of ADS-dedicated vehicles ("ADS-DVs") that lack manually operated driving controls. The regulatory barriers considered are those that pose unintended and unnecessary regulatory barriers, because the technical translation process does not change the performance standards of the FMVSS being considered.[91]

f) U.S. Department of Transportation Seeks Public Comment on Automated Driving System Safety Principles

On November 19, 2020, the DoT's National Highway Traffic Safety Administration ("NHTSA") announced that it is seeking public comment on the potential development of a framework of principles to govern the safe behavior of automated driving systems ("ADS") for use in connected and autonomous vehicles ("CAVs").[92] On the same day, NHTSA issued an advance notice of proposed rulemaking ("NPRM") on a possible ADS framework (the "ADS NPRM"). [93] The ADS NPRM sends a strong signal that vehicles with ADS may in future be subject to a new generation of performance and safety (as well as design) standards. For more details, please see our Legal Update: U.S. Department of Transportation Seeks Public Comment on Automated Driving System Safety Principles.

g) U.S. State Law

State regulatory activity has continued to accelerate, adding to the already complex mix of regulations that apply to companies manufacturing and testing AVs. As outlined in our 2019 Artificial Intelligence and Automated Systems Annual Legal Review, state regulations vary significantly.

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 AVs, 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.

Washington's HB 2676, which establishes minimum requirements for the testing of autonomous vehicles, went into effect on June 11, 2020. The bill requires companies testing AVs in Washington to report certain data regarding those tests to the state's Department of Licensing and to carry $5 million minimum in umbrella liability insurance.[94]

Also, in November 2020, Massachusetts voters approved a ballot initiative amending the Commonwealth's 2012 "Right to Repair Law." The amendment provides that motor vehicles sold in Massachusetts "with model year 2022" will be required to equip vehicles that use telematics systems—systems that collect and wirelessly transmit mechanical data to a remote server—with a standardized open access data platform. With authorization of the owner, telematics data will be available to independent repair facilities and dealerships not otherwise affiliated with the OEM of the vehicle, who will "send commands to, the vehicle for repair, maintenance, and diagnostic testing." Telematics data was purposefully excluded from the original law.[95]

2. European Commission Report on the Ethics of Connected and Automated Vehicles

In September 2020, the Commission published a report by an independent group of experts on the ethics of connected and automated vehicles ("CAVs").[96] The report—which promotes the "systematic inclusion of ethical considerations in the development and use of CAVs"[97]—sets out twenty ethical recommendations on road safety, privacy, fairness, AI explainability, responding to dilemma situations, clear testing guidelines and standards, the creation of a culture of responsibility for the development and deployment of CAVs, auditing CAV algorithmic decision-making reducing opacity, as well as the promotion of data, algorithm and AI literacy through public participation. The report applies a "Responsible Research and Innovation" approach that "recognises the potential of CAV technology to deliver the […] benefits [reducing the number of road fatalities and harmful emissions from transport, improving the accessibility of mobility services]" but also incorporates a broader set of ethical, legal and societal considerations into the development, deployment and use of CAVs and to achieve an "inherently safe design" based on a user-centric perspective.[98] The report builds on the Commission's strategy on Connected and Automated Mobility.[99]

3. Proposed German Legislation on Autonomous Driving

The German government intends to pass a law on autonomous vehicles ("Gesetz zum autonomen Fahren") by mid-2021.[100] The new law is intended to regulate the deployment of CAVs in specific operational areas by the year 2022 (including Level 5 "fully automated vehicles"), and will define the obligations of CAV operators, technical standards and testing, data handling, and liability for operators. The proposed law is described as a temporary legal instrument pending agreement on harmonized international regulations and standards.

Moreover, the German government also intends to create, by the end of 2021, a "mobility data room" ("Datenraum Mobilität"), described as a cloud storage space for pooling

mobility data coming from the car industry, rail and local transport companies, and private mobility providers such as car sharers or bike rental companies.[101] The idea is for these industries to share their data for the common purpose of creating more efficient passenger and freight traffic routes, and support the development of autonomous driving initiatives in Germany.

D. Intellectual Property

As AI systems evolve—producing "cultural artefacts, ranging from audio to text to images"[102]—intellectual property issues related to AI have 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.[103]

In 2020, the USPTO, United Kingdom Intellectual Property Office ("UKIPO"), and European Patent Office ("EPO") gave rulings on the questions of whether an AI system ("DABUS") could be named as the inventor on a patent application. All came to the same conclusion: existing law provides that an inventor must be a human.[104] Subsequently, the USPTO sought insight into public opinion on how intellectual property laws and policy should develop as AI technology advances, and issued a Request for Comment ("RFC") on August 27, 2019 (as reviewed in our client alert USPTO Requests Public Comments On Patenting Artificial Intelligence Inventions).

1. USPTO Report on Artificial Intelligence and Intellectual Property Policy

On October 6, 2020, the USPTO published a report "Public Views on Artificial Intelligence and Intellectual Property Policy" (the "Report").[105] The Report catalogs the roughly 200 comments received in response to the USPTO's RFC.[106] The USPTO requested feedback on issues such as whether current laws and regulations regarding patent inventorship and authorship of copyrighted work should be revised to take into account contributions other than by natural persons.

A general theme that emerged from the report was concern over the lack of a universally acknowledged definition of AI, and a majority view that current AI (i.e., AI that is not considered to be artificial general intelligence, or "AGI") can neither invent nor author without human intervention. The vast majority of commenters stated that no changes should be necessary to the current U.S. law—that only a natural person or a company (via assignment) should be considered the owner of a patent or an invention. Many commenters asserted that there are no patent eligibility considerations unique to AI Inventions, and that AI inventions should not be treated any differently than other computer-implemented inventions. This is consistent with how the USPTO currently examines AI inventions today: claims to an AI invention that fall within one of the four statutory categories and are patent-eligible under the *Alice/Mayo* test[107] will be patent subject matter-eligible under 35 U.S.C. § 101.

The comments also suggested that existing U.S. intellectual property laws are "calibrated correctly to address the evolution of AI" (although commenters were split as to whether any new classes of IP rights would be beneficial to ensure a more robust IP system), and that "human beings remain integral to the operation of AI, and this is an important consideration in evaluating whether IP law needs modification in view of the current state of AI technology."[108] Some commenters suggested that the USPTO should revisit the question when machines begin achieving AGI (i.e., when science agrees that machines can "think" on their own).

Finally, in response to a question about whether policies and practices of other global patent agencies should inform the USPTO's approach, there was a divide between commentators advocating for an evolution of global laws in a common direction, and those who cautioned against further attempts to harmonize international patent laws and procedures "because U.S. patent law is the gold standard."[109]

E. Financial Services

1. FINRA White Paper on AI

On June 12, 2020, the Financial Industry Regulatory Authority ("FINRA"), released a white paper on AI defining the scope of "AI" as it pertains to the securities industry, identifying areas in which broker-dealers are evaluating or using AI, and regulatory considerations for AI-based tools.[110]

The key areas in which the white paper contemplates AI being deployed are customer communications, investment processes, operational functions such as compliance and risk management, and administrative functions. FINRA notes that firms employing AI-based applications may "benefit from reviewing and updating their model risk management frameworks to address the new and unique challenges AI models may pose."

Notably, FINRA Rule 3110 requires firms to supervise activities relating to AI applications to ensure that the functions and outputs of the application are properly understood and in line with the firm's legal and compliance requirements. In addition, FINRA Rule 2010 requires firms to observe high standards of commercial honor and just and equitable principles of trade in the context of their AI applications. As such, FINRA recommends that firms review their data for potential biases and adopt data quality benchmarks and metrics as part of a comprehensive data governance strategy.

---

[1] Alex Engler, *6 developments that will define AI governance in 2021*, Brookings (Jan, 21, 2020), available at https://www.brookings.edu/research/6-developments-that-will-define-ai-governance-in-2021/.

[2] 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.

[3] UK Government, *Joint statement from founding members of the Global Partnership on Artificial Intelligence* (Jun. 15, 2020), available at https://www.gov.uk/government/publications/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence#fn:1.

[4] For further details, please see our 2019 Artificial Intelligence and Automated Systems Annual Legal Review.

[5] Robin Kelly, *Kelly, Hurd Introduce Bipartisan Resolution to Create National Artificial Intelligence Strategy* (Sept. 16, 2020), available at https://robinkelly.house.gov/media-center/press-releases/kelly-hurd-introduce-bipartisan-resolution-to-create-national-artificial?_sm_au_=iVV6kKLFkrjvZrvNFcVTvKQkcK8MG; H.Con.Res. 116, 116th Congress (2019-2020).

[6] Bipartisan Policy Center, *A National AI Strategy* (Sept. 1, 2020), available at https://bpcaction.org/wp-content/uploads/2020/09/1-Pager-on-National-AI-Strategy-Resolution-.pdf?_sm_au_=iVV6kKLFkrjvZrvNFcVTvKQkcK8MG.

[7] On September 10, 2020, the House Budget Committee held a hearing to discuss the impact of Artificial Intelligence on the U.S. economy, and specifically on what role technology should play in the country's recovery post-COVID-19. Witness Darrell West, Ph.D., of Brookings Institution warned that the rapid integration of AI technologies developed in the private sector could affect the American workforce by causing job losses and job dislocation.

[8] The 10 AI principles are: Public Trust in AI; Public Participation; Scientific Integrity and Information Quality; Risk Assessment and Management; Benefits and Costs; Flexibility; Fairness and Nondiscrimination; Disclosure and Transparency; Safety and Security; and Interagency Coordination.

[9] Director of the Office of Management and Budget, *Guidance for Regulation of Artificial Intelligence Applications* (Jan. 7, 2020), at 5, available at https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

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

[11] Director of the Office of Management and Budget, *Guidance for Regulation of Artificial Intelligence Applications* (Nov. 17, 2020), available at https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

[12] *Id*., Appendix A, at 12.

[13] *Id*., at 11; see also Appendix B: Template for Agency Plans, at 15-16.

[14] *Id*., at 2.

[15] David Shepherdson, *Trump signs order on principles for U.S. government AI use*, Reuters (Dec. 3, 2020), available at https://www.reuters.com/article/us-trump-ai/trump-signs-order-on-principles-for-u-s-government-ai-use-idUSKBN28D357; see also Stanford University, New York University, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* (Feb. 2020), available at https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf (documenting 157 use cases of AI by 64 U.S. federal agencies).

[16] For more detail, see our 2019 Artificial Intelligence and Automated Systems Annual Legal Review.

[17] NIST, *Four Principles of Explainable Artificial Intelligence* (Aug. 2020), NISTIR 8312, available at https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable%20AI%20Draft%20NISTIR8312%20%281%29.pdf.

[18] H.R. 6395, 116th Congress (2019-2020).

[19] For more details, see our 2019 Artificial Intelligence and Automated Systems Annual Legal Review and Artificial Intelligence and Automated Systems Legal Update (2Q20).

[20] The Artificial Intelligence for the Armed Forces Act (S. 3965); the National AI Research Resource Task Force Act (H.R. 7096 and S. 3890); the Deepfakes Report Act (S. 2065), which was passed as a standalone bill in the Senate on October 24, 2019; and the Artificial Intelligence Education Act (H.R. 8390). For additional detail on these bills, see our previous 2020 Legal Updates (1Q20, 2Q20 and 3Q20).

[21] Stanford University, hai, *Summary of AI Provisions from the National Defense*

Authorization Act 2021, available at https://hai.stanford.edu/policy/policy-resources/summary-ai-provisions-national-defense-authorization-act-2021.

[22] H.R. 6395, Title II, Sec. 235.

[23] *Id*., Title LI, Sec. 5102

[24] *Id*., Title LI, Sec. 5103

[25] Stanford University, *Summary of AI Provisions from the National Defense Authorization Act 2021*, *supra* n.21.

[26] H.R. 6395, Title LI, Sec. 5104.

[27] Stanford University, *Summary of AI Provisions from the National Defense Authorization Act 2021*, *supra* n.21.

[28] H.R. 6395, Title LI, Sec. 5106.

[29] *Id*., Title LII, Sec. 5201.

[30] *Id*., Title LIII, Sec. 5301.

[31] Stanford University, *Summary of AI Provisions from the National Defense Authorization Act 2021*, *supra* n.21.

[32] Comm. Sci. Space & Tech., *Lucas Introduces Comprehensive Legislation to Secure American Leadership in Science and Technology* (Jan. 29, 2020), available at https://republicans-science.house.gov/news/press-releases/lucas-introduces-comprehensive-legislation-secure-american-leadership-science.

[33] H.R. 6950, 116th Cong (2019–2020).

[34] H.R. 2575, 116th Congress (2019-2020).

[35] The Ripon Advance, *GOP senators praise House passage of AI in Government Act* (Sept. 16, 2020), available at https://riponadvance.com/stories/gop-senators-praise-house-passage-of-ai-in-government-act/?_sm_au_=iVV6kKLFkrjvZrvNFcVTvKQkcK8MG; Rob Portman, *House Passes Portman, Gardner Bipartisan Legislation to Improve Federal Government's Use of Artificial Intelligence* (Sept. 14, 2020), *available at* https://www.portman.senate.gov/newsroom/press-releases/house-passes-portman-gardner-bipartisan-legislation-improve-federal?_sm_au_=iVV6kKLFkrjvZrvNFcVTvKQkcK8MG.

[36] 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.

[37] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[38] *Id*. Industries in critical sectors include healthcare, transport, police, recruitment, and the legal system, while technologies of critical use include such technologies with a risk of death, damage or injury, or with legal ramifications.

[39] European Commission, *A European strategy for data*, COM (2020) 66 (Feb. 19,

2020), available at https://ec.europa.eu/info/files/communication-european-strategy-data_en.

[40] European Commission, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM (2020) 64 (Feb. 19, 2020), available at https://ec.europa.eu/info/files/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics_en.

[41] *Innovative And Trustworthy AI: Two Sides Of The Same Coin*, Position paper on behalf of Denmark, Belgium, the Czech Republic, Finland, France, Estonia, Ireland, Latvia, Luxembourg, the Netherlands, Poland, Portugal, Spain and Sweden, available at https://em.dk/media/13914/non-paper-innovative-and-trustworthy-ai-two-side-of-the-same-coin.pdf; see also https://www.euractiv.com/section/digital/news/eu-nations-call-for-soft-law-solutions-in-future-artificial-intelligence-regulation/.

[42] Stellungnahme der Bundesregierung der Bundesrepublik Deutschland zum Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM (2020) 65 (June 29, 2020), available at https://www.ki-strategie-deutschland.de/files/downloads/Stellungnahme_BReg_Weissbuch_KI.pdf; see also Philip Grüll, *Germany calls for tightened AI regulation at EU level*, Euractiv (July 1, 2020), available at https://www.euractiv.com/section/digital/news/germany-calls-for-tightened-ai-regulation-at-eu-level/. Note also that German lawmaker Axel Voss has been appointed rapporteur of the European Parliament's Special Committee on Artificial Intelligence in a Digital Age ("AIDA"), and will be in charge of drafting reports by the committee setting out EU goals and recommendations for AI.

[43] European Commission, *White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trust*, COM (2020) (July 17, 2020), available at https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence.

[44] European Commission, *Artificial intelligence – ethical and legal requirements,* COM (2020) (June 2020), available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence.

[45] *Id*.

[46] European Parliament, *Setting up a special committee on artificial intelligence in a digital age, and defining its responsibilities, numerical strength and term of office* (June 18, 2020), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0162_EN.html; the European Parliament is also working on a number of other issues related to AI, including: the civil and military use of AI (legal affairs committee); AI in education, culture and the audio-visual sector (culture and education committee); and the use of AI in criminal law (civil liberties committee).

[47] European Parliament, News Report, *AI rules: what the European Parliament wants* (Oct. 21, 2020), available at https://www.europarl.europa.eu/news/en/headlines/society/20201015STO89417/ai-rules-what-the-european-parliament-wants.

[48] European Parliament, *Parliament leads the way on first set of EU rules for Artificial Intelligence* (Oct. 20, 2020), available at https://www.europarl.europa.eu/news/en/press-room/20201016IPR89544/.

[49] In addition, the European Parliament announced that it had approved two separate legislative initiative reports calling on the Commission to address and tackle current shortcomings in the online environment in its Digital Services Act ("DSA") package, due to

be presented in December 2020. In particular, the Parliament noted that the EU aims to shape the digital economy at the EU level, as well as set the standards for the rest of the world. In addition, the Parliament outlined in its reports that all digital service providers established in non-EU must adhere to the DSA's rules when their services are also aimed at consumers or users in the EU.

[50] European Parliament, *Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies* (2020/2012 (INL)) (Oct. 8, 2020), available at https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.pdf; European Parliament, *Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies* (2020/2012 (INL)) (Oct. 20, 2020), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.pdf.

[51] Press Release, European Parliament, *Parliament leads the way on first set of EU rules for Artificial Intelligence* (Oct. 20, 2020), available at https://www.europarl.europa.eu/news/en/press-room/20201016IPR89544/.

[52] *Id*.

[53] Press Release, European Parliament, *Parliament leads the way on first set of EU rules for Artificial Intelligence* (Oct. 20, 2020), available at https://www.europarl.europa.eu/news/en/press-room/20201016IPR89544/.

[54] European Parliament, *Report with recommendations to the Commission on a civil liability regime for artificial intelligence* (2020/2014 (INL)) (Oct. 5, 2020), available at https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_EN.pdf; European Parliament, *Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence* (2020/2014 (INL)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.pdf;

[55] European Parliament, *Report on intellectual property rights for the development of artificial intelligence technologies* (2020/2015(INI)) (Oct. 2, 2020), available at https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.pdf; European Parliament, *Resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies* (2020/2015(INI)) (Oct. 20, 2020), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.pdf.

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

[57] AI HLEG, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment* (Jul. 17 2020), available at https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[58] Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study (Dec. 17, 2020), available at https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da.

[59] Deutscher Bundestag, Enquete-Kommission, Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale, *Kurzzusammenfassung des Gesamtberichts* (Oct. 28, 2020), available at https://www.bundestag.de/resource/blob/801584/102b397cc9dec49b5c32069697f3b1e3/Kurzfassung-des-Gesamtberichts-data.pdf.

[60] Committee on Standards in Public Life, *Artificial Intelligence and Public Standards: report* (Feb. 10, 2020), available at https://www.gov.uk/government/publications/artificial-

intelligence-and-public-standards-report.

[61] Centre for Data Ethics and Innovation, *AI Barometer Report* (June 2020), available at https://www.gov.uk/government/publications/cdei-ai-barometer/cdei-ai-barometer

[62] UK Government, AI Council's *AI Roadmap* (Jan. 6, 2021), available at https://www.gov.uk/government/publications/ai-roadmap.

[63] *Id*., at 24.

[64] house of lords Liaison Committee, *AI in the UK: No Room for Complacency*, 7th Rep. of Session 2019-21 (Dec. 18, 2020), available at https://publications.parliament.uk/pa/ld5801/ldselect/ldliaison/196/196.pdf.

[65] UK ICO, *Guidance on AI and data protection* (July 30, 2020), available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/.

[66] Examples of such privacy-enhancing techniques include perturbation or adding 'noise', synthetic data, and federated learning.

[67] On the topic of data minimization, see also the European Data Protection Board's ("EDPB") Draft Guidelines on the Principles of Data Protection by Design and Default under Article 25 of the GDPR, adopted on October 20, 2020 after a public consultation and available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[68] *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.

[69] Letter to the Hon. Janet Dhillon, Chair of EEOC (Dec. 8, 2020), available at https://www.bennet.senate.gov/public/_cache/files/0/a/0a439d4b-e373-4451-84ed-ba333ce6d1dd/672D2E4304D63A04CC3465C3C8BF1D21.letter-to-chair-dhillon.pdf.

[70] A.B. 2269, 2019-2020 Reg. Sess. (Cal. 2020).

[71] *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.

[72] For more details, see our 2019 Artificial Intelligence and Automated Systems Annual Legal Review.

[73] S. 3284, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3284.

[74] *E.g.,* Idaho's Facial Recognition Technology Act, H.B. 492; Maryland's Facial Recognition Privacy Protection Act, H.B. 1578; Louisiana's Act Relative to Facial Recognition Software, H.B. 662; Portland, Oregon's

[75] Ordinance No. 190114, Title 34 Digital Justice, Chapter 34.10, "Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland". The City Council also passed a separate ordinance banning the use of facial recognition technology by the city government (including local police)

[76] The prohibition does not apply to use of face recognition technologies to the extent necessary for a private entity to comply with federal, state, or local laws; for user verification purposes by an individual to access the individual's own personal or employer issued communication and electronic devices; or in automatic face detection services in social media applications. See 34.10.040

[77] H.B. 1202(a)(3).

[78] For more details, see Gibson Dunn's Artificial Intelligence and Automated Systems Legal Update (1Q20).

[79] Letter from Jay Inslee, Governor of the State of Washington, to The Senate of the State of Washington (March 31, 2020), available at https://crmpublicwebservice.des.wa.gov/bats/attachment/vetomessage/559a6f89-9b73-ea11-8168-005056ba278b#page=1.

[80] 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.

[81] 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.

[82] U.S. Dep't of Transp., NHTSA Issues First-Ever Proposal to Modernize Occupant Protection Safety Standards for Vehicles Without Manual Controls, available at https://www.nhtsa.gov/press-releases/adapt-safety-requirements-ads-vehicles-without-manual-controls.

[83] 49 CFR 571 2020, available at https://www.federalregister.gov/documents/2020/03/30/2020-05886/occupant-protection-for-automated-driving-systems.

[84] H.R. __ 116th Congress (2019-2020).

[85] For more information, please see our legal updates Accelerating Progress Toward a Long-Awaited Federal Regulatory Framework for Autonomous Vehicles in the United States and 2019 Artificial Intelligence and Automated Systems Annual Legal Review.

[86] Energy & Commerce Committee Republicans, Press Release, *E&C Republicans Continue Leadership on Autonomous Vehicles* (Sept. 23, 2020), available at https://republicans-energycommerce.house.gov/news/press-release/ec-republicans-continue-leadership-on-autonomous-vehicles/.

[87] U.S. Dep't of Transp., U.S. Transportation Secretary Elaine L. Chao Announces First Participants in New Automated Vehicle Initiative to Improve Safety, Testing, and Public Engagement (June 15, 2020*), available at* https://www.nhtsa.gov/press-releases/participants-automated-vehicle-transparency-and-engagement-for-safe-testing-initiative.

[88] U.S. Dep't of Transp., av test Initiative, available at https://www.nhtsa.gov/automated-vehicles-safety/av-test.

[89] *See, e.g.*, Keith Laing, *Michigan, Fiat Chrysler Join Federal Self-Driving Car Initiative*, The Detroit News (June 15, 2020), available at https://www.detroitnews.com/story/business/autos/2020/06/15/michigan-fiat-chrysler-join-federal-self-driving-car-initiative/3194309001/.

[90] Blanco, M., Chaka, M., Stowe, L., Gabler, H. C., Weinstein, K., Gibbons, R. B., Fitchett, V. L. (2020, April). FMVSS considerations for vehicles with automated driving systems: Volume 1 (Report No. DOT HS 812 796), U.S. Dep't of Transp., available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/ads-dv_fmvss_vol1-042320-v8-tag.pdf.

[91] *Id*. at vii.

[92] U.S. Dep't of Transp., Press Release, *U.S. Department of Transportation Seeks Public Comment on Automated Driving System Safety Principles* (Nov. 19, 2020), available at https://www.nhtsa.gov/press-releases/public-comment-automated-driving-system-safety-principles.

[93] Framework for Automated Driving System Safety, 49 Fed. Reg. 571 (Nov. 19, 2020), available here.

[94] H.B. 2676, Washington State Legislature, available at https://apps.leg.wa.gov/billsummary/?BillNumber=2676&Year=2020&Initiative=false.

[95] *See* Rob Stumpf, *There's Another Huge Right to Repair Fight Brewing in Massachusetts*, The Drive (Oct. 13, 2020), available at https://www.thedrive.com/news/36980/theres-another-huge-right-to-repair-fight-brewing-in-massachusetts.

[96] European Commission, Press Release, *New recommendations for a safe and ethical transition towards driverless mobility*, COM (2020) (Sept. 18, 2020), available at https://ec.europa.eu/info/news/new-recommendations-for-a-safe-and-ethical-transition-towards-driverless-mobility-2020-sep-18_en.

[97] *Id*.

[98] European Commission, Directorate-General for Research and Innovation, Independent Expert Report, *Ethics of Connected and Automated Vehicles: Recommendations on road safety, privacy, fairness, explainability, and responsibility* (Sept. 18, 2020), at 4, available *here*.

[99] EC, *Connected and automated mobility in Europe*, COM(2020) (June 22, 2020), available *at* https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe.

[100] Bundesministerium für Verkehr und digitabe Infrastruktur, Gesetz zum autonomen Fahren (Oct. 2020), available at https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html ; see also Josef Erl, *Autonomes Fahren: Deutschland soll Weltspitze werden*, Mixed.de (Oct. 31, 2020), available at https://mixed.de/autonomes-fahren-deutschland-soll-weltspitze-werden/.

[101] Daniel Delhaes, *Deutsche Autoindustrie erwägt, ihre Datenschätze zu bündeln*, Handelsblatt (July 9, 2020), available at https://www.handelsblatt.com/technik/sicherheit-im-netz/autonomes-fahren-deutsche-autoindustrie-erwaegt-ihre-datenschaetze-zu-buendeln/26164062.html?ticket=ST-2824809-tuIGjXYQywf7MHzRurpa-ap4.

[102] Jack Clark, *ImportAI* (Jan. 18, 2021), available at https://jack-clark.net/.

[103] *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.

[104] *See* Decision on Petition re App'n No. 16/524,350 (USPTO, April 27, 2020); Decision on Petition re App'n Nos. GB1816909.4 and GB1818161.0 (UKIPO, December 4, 2019); *Stephen L Thaler v The Comptroller-General of Patents, Designs And Trade Marks* [2020] EWHC 2412 (Pat); Press Release, European Patent Office, *EPO publishes grounds for its decision to refuse two patent applications naming a machine as inventor* (January 28, 2020), available at https://www.epo.org/news-events/news/2020/20200128.html.

[105] United States Patent and Trademark Office, *USPTO releases report on artificial intelligence and intellectual property policy* (Oct. 6, 2020), available at https://www.uspto.gov/about-us/news-updates/uspto-releases-report-artificial-intelligence-and-intellectual-property?_sm_au_=iVV6kKLFkrjvZrvNFcVTvKQkcK8MG. For more detail, see our Artificial Intelligence and Automated Systems Legal Update (3Q20).

[106] United States Patent and Trademark Office, *Public Views on Artificial Intelligence and Intellectual Property Policy* (Oct. 2020), available at https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf. On October 30, 2019, the USPTO also issued a request for comments on Intellectual Property Protection for Artificial Intelligence Innovation, with respect to IP policy areas other than patent law. The October 2020 USPTO publication summarizes the responses by commentators at Part II from p. 19 of the Report onwards.

[107] *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 221 (2014); *Mayo Collaborative Servs. v. Prometheus Labs., Inc*., 566 U.S. 66 (2012).

[108] *Id*. at ii.

[109] *Id*. at 18.

[110] finra, *Artificial Intelligence (AI) in the Securities Industry* (June 20, 2020), available at https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf.

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Frances Waldmann, Haley Morrisson, Tony Bedel, Emily Lamm and Derik Rao.

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)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33 180, kgesing@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)
Christopher T. Timura - Washington, D.C. (+1 202-887-3690, ctimura@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)

Related Capabilities

Artificial Intelligence