GIBSON DUNN

Artificial Intelligence and Automated Systems Legal Update (1Q21)

Client Alert | April 23, 2021

Regulatory and policy developments during the first quarter of 2021 reflect a global tipping point toward serious regulation of artificial intelligence ("AI") in the U.S. and European Union ("EU"), with far-reaching consequences for technology companies and government agencies.[1] In late April 2021, the EU released its long-anticipated draft regulation for the use of AI, banning some "unacceptable" uses altogether and mandating strict guardrails such as documentary "proof" of safety and human oversight to ensure AI technology is "trustworthy."

While these efforts to aggressively police the use of AI will surprise no one who has followed policy developments over the past several years, the EU is no longer alone in pushing for tougher oversight at this juncture. As the United States' national AI policy continues to take shape, it has thus far focused on ensuring international competitiveness and bolstering national security capabilities. However, as the states move ahead with regulations seeking accountability for unfair or biased algorithms, it also appears that federal regulators—spearheaded by the Federal Trade Commission ("FTC")—are positioning themselves as enforcers in the field of algorithmic fairness and bias.

Our 1Q21 Artificial Intelligence and Automated Systems Legal Update focuses on these critical regulatory efforts, and also examines other key developments within the U.S. and Europe that may be of interest to domestic and international companies alike. As a result of several significant developments in April, and to avoid the need for multiple alerts, this 1Q21 update also include a number of matters from April, the beginning of 2Q21.

Related People

Kai Gesing

Christopher T. Timura

Frances Waldmann

Prachi Mistry

Table of Contents

I. U.S. NATIONAL POLICY & REGULATORY DEVELOPMENTS

A. U.S. National AI Strategy

The U.S. federal government's national AI strategy continues to take shape, bridging the old and new administrations. Pursuant to the National AI Initiative Act of 2020, which was passed on January 1 as part of the National Defense Authorization Act of 2021 ("NDAA"),[2] the White House Office of Science and Technology Policy ("OSTP") formally established the National AI Initiative Office (the "Office") on January 12. The Office—one of several new federal offices mandated by the NDAA—will be responsible for overseeing and implementing a national AI strategy and acting as a central hub for coordination and collaboration by federal agencies and outside stakeholders across government, industry and academia in AI research and policymaking.[3]

Further, on January 27, President Biden signed a memorandum titled "Restoring trust in government through science and integrity and evidence-based policy making," setting in motion a broad review of federal scientific integrity policies and directing agencies to bolster their efforts to support evidence-based decision making. The President designated the OSTP to constitute an interagency Task Force to carry out the review,[4] which must be completed within 120 days of appointment of the Task Force members[5] and is expected to "generate important insights and best practices including transparency and accountability…."[6] On the same day, the President also signed an executive order to formally reconstitute the President's Council of Advisors on Science and Technology.[7]

B. National Security & Trade

1. *New House Subcommittee on Cyber, Innovative Technologies, and Information Systems*

In February 2021, the House Armed Services Committee created a new Subcommittee on Cyber, Innovative Technologies, and Information Systems ("CITI") out of the former Intelligence and Emerging Threats and Capabilities Subcommittee.[8] CITI will provide focused oversight on technology matters, including cybersecurity, IT policy, AI, electronic warfare and software acquisition, and shift non-technical topics, such as special operations and counter-proliferation of weapons of mass destruction, to other lawmakers. On March 12, the Subcommittee held a joint hearing with the House Committee on Oversight and Reform's Subcommittee on National Security to receive testimony from the National Security Commission on Artificial Intelligence on the Commission's final report (discussed in more detail below).[9]

2. *NSCAI Final Report*

The National Defense Authorization Act of 2019 created a 15-member National Security Commission on Artificial Intelligence ("NSCAI"), and directed that the NSCAI "review and advise on the competitiveness of the United States in artificial intelligence, machine learning, and other associated technologies, including matters related to national security, defense, public-private partnerships, and investments."[10] Over the past two years, NSCAI has issued multiple reports, including interim reports in November 2019 and October 2020, two additional quarterly memorandums, and a series of special reports in response to the COVID-19 pandemic.[11]

On March 1, 2021, the NSCAI submitted its Final Report to Congress and to the President. At the outset, the report makes an urgent call to action, warning that the U.S.

government is presently not sufficiently organized or resourced to compete successfully with other nations with respect to emerging technologies, nor prepared to defend against AI-enabled threats or to rapidly adopt AI applications for national security purposes. Against that backdrop, the report outlines a strategy to get the United States "AI-ready" by 2025.[12] The Commission explains:

The United States should invest what it takes to maintain its innovation leadership, to responsibly use AI to defend free people and free societies, and to advance the frontiers of science for the benefit of all humanity. AI is going to reorganize the world.

America must lead the charge.

The more than 700-page report consists of two parts: Part I, "Defending America in the AI Era," makes recommendations on how the U.S. government can responsibly develop and use AI technologies to address emerging national security threats, focusing on AI in warfare and the use of autonomous weapons, AI in intelligence gathering, and "upholding democratic values in AI." The report's recommendations identify specific steps to improve public transparency and protect privacy, civil liberties and civil rights when the government is deploying AI systems. NSCAI specifically endorses the use of tools to improve transparency and explainability: AI risk and impact assessments; audits and testing of AI systems; and mechanisms for providing due process and redress to individuals adversely affected by AI systems used in government. The report also recommends establishing governance and oversight policies for AI development, which should include "auditing and reporting requirements," a review system for "high-risk" AI systems, and an appeals process for those affected.

Part II, "Winning the Technology Competition," outlines urgent actions the government must take to promote AI innovation to improve national competitiveness, secure talent, and protect critical U.S. advantages, including IP rights. The report highlights how stringent patent eligibility requirements in U.S. courts, particularly with respect to computer-implemented and biotech-related inventions, and a lack of explicit legal protections for data have created uncertainty in IP protection for AI innovations, discouraging the pursuit of AI inventions and hindering innovation and collaboration. NSCAI also notes that China's significant number of patent application filings have created a vast reservoir of "prior art" and caused the USPTO's patent examination process increasingly difficult. As such, the report recommends that the President issue an executive order to recognize IP as a national priority, and develop a comprehensive plan to reform IP policies to incentivize and protect AI and other emerging technologies.[13]

The NSCAI report may provide opportunity for legislative reform, which would spur investments in AI technologies and accelerate government adoption of AI technologies in national security. The report's recommendations with respect to transparency and explainability may also have significant implications for potential oversight and regulation of AI in the private sector.

3. *Executive Order on U.S. Supply Chains*

At the end of February, the Biden Administration issued a sweeping executive order launching a year-long, multi-agency review of several sectors, including several that will be critical to maintaining U.S. leadership in the development of AI and associated technologies. The purpose of the "America's Supply Chains" Executive Order 14017, as President Biden puts it, is to "help address the vulnerabilities in our supply chains across . . . critical sectors of our economy so that the American people are prepared to withstand any crisis." The Executive Order has put into motion 100-day reviews of four types of products by four different federal agencies: (1) semiconductors (Commerce); (2) high-capacity batteries, including electric-vehicle batteries (Energy); (3) critical minerals and strategic materials, such as rare earth elements (Defense); and (4) pharmaceuticals and their active ingredients (Health and Human Services). Executive Branch work to implement the E.O. is being coordinated by the Assistant to the President for National

Security Affairs (APNSA) and the Assistant to the President for Economic Policy (APEP). By February 24, 2022, the Secretaries of Defense, Health and Human Services, Commerce and Homeland Security, Energy, Transportation, and Agriculture are to provide the President with broader and deeper assessments of the defense industrial base, the public health and biological preparedness industrial base, the information and communications industrial base, energy sector industrial base, transportation industrial base, and agricultural commodities and food products industrial base, respectively.

The Biden Administration's prioritization of semiconductors and critical minerals and strategic materials in the 100-day review was expected; they are critical links in many supply chains and either already are or could be in short supply to the United States for a range of reasons. Both are of specific relevance to the raw materials and manufacturing supply chains that support AI development and applications. Especially in light of ongoing geopolitical and economic tensions between the United States and China, the potential inability of the U.S. to access supply of critical minerals from China and many U.S. companies' dependence on only a small handful of advanced semiconductor manufacturers based in Austria, Germany, Japan, The Netherlands, South Korea, Taiwan and the United States for critical links in their supply chains makes the advanced semiconductor supply chain especially prone to disruption.

Agency action has already begun with respect to the 100-day review of semiconductors. On March 11, the Commerce Department's Bureau of Industry and Security (BIS) issued a notice seeking public comment on risks in the semiconductor manufacturing and advanced packaging supply chains. The notice requested information on a range of supply issues including the critical and essential goods and materials required for semiconductor manufacturing and advanced packaging support chain, manufacturing capabilities, and key skill sets and personnel necessary to sustain the U.S. semiconductor ecosystem. BIS also sought comments on how a failure to sustain the semiconductor supply chain might impact "key downstream capabilities," including artificial intelligence applications. BIS received 34 comments by the comment due date of April 5 from a range of private sector companies, trade associations, universities, and individuals. In addition to the written comments, BIS also convened a virtual public forum inviting speakers to provide further input on the questions presented in its notice on April 8.

Although the focus of the America's Supply Chain EO is on executive agency reporting, we expect the EO to provide U.S. private and non-governmental sectors significant opportunities for agency engagement. To state the obvious, the U.S. does not have a centralized planned economy, and U.S. Executive Branch agencies often lack the visibility required to produce reports that accurately reflect the state of play in many international supply chains. Especially because identified gaps and weak links in strategic supply chains are likely to be a focus of targeted infrastructure spending, tax incentives, export controls, immigration reform, and other regulatory action during the Biden Administration, many of our clients could find it well worth the effort to participate in agency information gathering like BIS's public comment process, either directly or indirectly through trade associations.

Scrutiny on semiconductor supply chains has not been limited to the Executive Branch, however, and a recent request from Congress illustrates how even individual transactions involving specific links in the semiconductor supply may become subject to regulatory action as Commerce and other U.S. agencies develop a deeper understanding of supply chain dynamics. On March 19, 2021, two Republican lawmakers sent a letter to the Commerce Secretary to prevent ASML Holdings NV, a Dutch technology firm, from supplying critical systems to Semiconductor Manufacturing International Corp. ("SMIC"), a Chinese chipmaker. Sen. Marco Rubio (R-FL) and Rep. Michael McCaul (R-Texas) said that the U.S. should exercise its diplomatic leverage to weaken China's foothold in the semiconductor industry. The lawmakers also asked Commerce Secretary Raimondo to add SMIC to the Commerce Department's Entity List, which would limit SMIC's ability to source materials even for those that are not manufactured in the United States. The two

lawmakers proposed that a presumption of denial apply in the export licensing process to any China-facing export “capable of producing” chips smaller than 16 nanometers, which would broaden the scope of the products subject to the presumption of denial. The Commerce Secretary has not responded to the letter or issued any statement regarding the letter to date.

4. *Interim Final Rule “Securing the Information and Communications Technology and Services (“ICTS”) Supply Chain”*

The Department of Commerce also has taken the next step in implementing another Executive Order, this time from the Trump Administration, focused on the ICTS Supply Chain. An Interim Final Rule implementing the EO became effective on March 22, 2021.[14] The ICTS EO is an effort to protect against threats posed on the use of hardware, software and services designed, developed, manufactured or supplied by companies owned by, controlled by, or subject to the direction or control of China and other “foreign adversary” countries, but has been the target of consternation by commentators since its issuance on May 15, 2019.

The Interim Final Rule implements the Secretary of Commerce’s new power to prohibit transactions which involve the *acquisition, importation, transfer, installation, dealing in, or usage of* certain ICTS.[15] Transactions subject to the Secretary of Commerce’s review and prohibition include those involving managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download. Any of these actions can be prohibited or subject to licensing driven mitigation when the services, equipment, or software is designed, developed, manufactured, or supplied by companies owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, and poses an undue or unacceptable risk.[16]

Many different AI-related transactions could be impacted by the ICTS transaction review. Not only does the Interim Final Rule specifically include ICTS infrastructure that is integral to AI and machine learning technologies among the transactions it deems ICTS transactions, but it also includes other kinds of transactions that are necessary to support AI development or deployment, including certain software, hardware, or any other product or services integral to data hosting or computing services, and certain ICTS products, such as internet-enabled sensors, webcams, routers, modems, drones, or any other end-point surveillance or monitoring device, home networking device, or aerial system. Thus, companies in the U.S. seeking to store training data or use the processing power of cloud services to develop or host AI applications could see their access to China-based or China company-owned or controlled cloud service providers now subject to Department of Commerce licensing. Similarly, companies already deploying devices that make use of AI could find their ability to source cheap parts and components from foreign advisory companies limited by a transaction review.

C. Algorithmic Accountability and Consumer Safety

Companies using algorithms, automated processes, and/or AI-enabled applications are now squarely on the radar of both federal and state regulators and lawmakers. In 2020, a number of draft federal bills and policy measures addressing algorithmic accountability and transparency had hinted at a sea change amid growing public awareness of AI’s potential to pose a risk to consumers, including by creating harmful bias. While no AI-specific federal legislation has been enacted to date, federal regulators, including the FTC, have now signaled that they will not wait to bring enforcement actions. Moreover, a steady increase in state privacy laws has placed increasing focus on governance of the biometric data utilized by facial recognition technologies. The past quarter saw a number of developments that suggest companies using facial recognition technology may be subject to stricter regulation and enforcement with respect to the use and retention of biometric identifiers extracted from facial images at both federal and state level.[17]

1. *Algorithmic Fairness*

a) FTC Statement Announces Intent to Take Enforcement Action Against "Biased" Algorithms

On April 19, the FTC published a blog post, "Aiming for truth, fairness, and equity in your company's use of AI," announcing the Commission's intent to bring enforcement actions related to "biased algorithms" under section 5 of the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act.[18] Notably, the statement expressly notes that " the sale or use of – for example – racially biased algorithms" falls within the scope of the prohibition of unfair or deceptive business practices.

The FTC also provides some concrete guidance on "using AI truthfully, fairly, and equitably," indicating that it expects companies to "do more good than harm" by auditing its training data and, if necessary, "limit[ing] where or how [they] use the model;" testing its algorithms for improper bias before and during deployment; employing transparency frameworks and independent standards; and being transparent with consumers and seeking appropriate consent to use consumer data. The guidance also warns companies against making statements to consumers that "overpromise" or misrepresent the capabilities of a product, noting that biased outcomes may be considered deceptive and lead to FTC enforcement actions.

This statement of intent comes on the heels of remarks by Acting FTC Chairwoman Rebecca Kelly Slaughter on February 10 at the Future of Privacy Forum, previewing enforcement priorities under the Biden Administration and specifically tying the FTC's role in addressing systemic racism to the digital divide, exacerbated by COVID-19, AI and algorithmic decision-making, facial recognition technology, and use of location data from mobile apps.[19] It also follows the FTC's informal guidance last year outlining principles and best practices surrounding transparency, explainability, bias, and robust data models.[20]

The FTC's stance has bipartisan support in the Senate, where FTC Commissioner Rohit Chopra provided a statement on April 20, noting that "Congress and the Commission must implement major changes when it comes to stopping repeat offenders" and that "since the Commission has shown it often lacks the will to enforce agency orders, Congress should allow victims and state attorneys general to seek injunctive relief in court to halt violations of FTC orders."[21]

We recommend that companies developing or deploying automated decision-making adopt an "ethics by design" approach and review and strengthen internal governance, diligence and compliance policies. Companies should also stay abreast of developments concerning the FTC's ability to seek restitution and monetary penalties[22] and impose obligations to delete algorithms, models or data (a potential new remedial obligation that is addressed in more detail below).

b) Bipartisan U.S. Lawmakers Introduce Bill Banning Law Enforcement Agencies from Accessing Illegally Obtained User Data

On April 21, a bipartisan group of lawmakers introduced a bill banning law enforcement agencies from buying access to user data from "data brokers," including companies that "illegitimately obtained" their records.[23] The bill, titled "The Fourth Amendment Is Not For Sale Act," is sponsored by a bipartisan group including Sen. Ron Wyden (D-OR), Sen. Rand Paul (R-KY) and 18 other members of the Senate, and purports to close "major loopholes in federal privacy law."[24] The bill would force law enforcement agencies to obtain a court order before accessing users' personal information through third-party brokers—companies that aggregate and sell personal data like detailed user location—and prevents law enforcement and intelligence agencies buying data that was "obtained from a user's account or device, or via deception, hacking, violations of a contract, privacy policy, or terms of service."[25] Reps. Jerry Nadler (D-NY) and Zoe Lofgren (D-CA)

introduced a companion bill in the House.

c) Washington State Lawmakers Introduce a Bill to Regulate AI, S.B. 5116

On the heels of Washington's landmark facial recognition bill (S.B. 6280) enacted last year,[26] state lawmakers and civil rights advocates proposed new rules to prohibit discrimination arising out of automated decision-making by public agencies.[27] The bill, which is sponsored by Sen. Bob Hasegawa (D-Beacon Hill), would establish new regulations for government departments that use "automated decisions systems," a category that includes any algorithm that analyzes data to make or support government decisions.[28] If enacted, public agencies in Washington state would be prohibited from using automated decision systems that discriminate against different groups or make final decisions that impact the constitutional or legal rights of a Washington resident. The bill also bans government agencies from using AI-enabled profiling in public spaces. Publicly available accountability reports ensuring that the technology is not discriminatory would be required before an agency can use an automated decision system. The bill has been referred to Ways & Means.

2. *Facial Recognition*

a) FTC Enforcement

In January 2021, the Federal Trade Commission ("FTC") announced its settlement with Everalbum, Inc. in relation to its "Ever App," a photo and video storage app that used facial recognition technology to automatically sort and "tag" users' photographs.[29] The FTC alleged that Everalbum made misrepresentations to consumers about its use of facial recognition technology and its retention of the photos and videos of users who deactivated their accounts in violation of Section 5(a) of the FTC Act. Pursuant to the settlement agreement, Everalbum must delete models and algorithms that it developed using users' uploaded photos and videos and obtain express consent from its users prior to applying facial recognition technology, underscoring the emergence of deletion as a potential enforcement measure. A requirement to delete data, models and algorithms developed by using data collected without express consent could represent a significant remedial obligation with broader implications for AI developers.

Signaling the potential for increasing regulation and enforcement in this area, FTC Commissioner Rohit Chopra issued an accompanying statement describing the settlement as a "course correction," commenting that facial recognition technology is "fundamentally flawed and reinforces harmful biases" while highlighting the importance of "efforts to enact moratoria or otherwise severely restrict its use." However, the Commissioner also cautioned against "broad federal preemption" on data protection and noted that the authority to regulate data rights should remain at state-level.[30] We will carefully monitor any further enforcement action by the FTC (and other regulators), and recommend that companies developing or using facial recognition technologies seek specific legal advice with respect to consent requirements around biometric data as well as robust AI diligence and risk-assessment process for third-party AI applications.

b) Virginia Passes Ban on Law Enforcement Use of Facial Recognition Technology, H.B. 2031

The legislation, which won broad bipartisan support, prohibits all local law enforcement agencies and campus police departments from purchasing or using facial recognition technology unless it is expressly authorized by the state legislature.[31] The law will take effect on July 1, 2021. Virginia joins California, as well as numerous cities across the U.S., in restricting the use of facial recognition technology by law enforcement.[32]

c) BIPA

i. Litigation

On March 15, 2021, Judge James L. Robart of the U.S. District Court for the Western District of Washington declined to dismiss two putative class action suits accusing two technology companies of violating Illinois residents' privacy rights under BIPA.[33] The nearly identical complaints alleged that the companies violated BIPA by using a data set compiled by IBM containing geometric scans of their faces without their permission. The court found that plaintiffs' claims could proceed under Sections 15(b) and 15(c) of BIPA.

On March 16, 2021, Illinois District Judge Sara L. Ellis dismissed proposed class claims against Clarifai, Inc., a facial recognition software maker, under BIPA.[34] The Complaint alleged that Clarifai was harvesting facial data from OkCupid dating profile photos without obtaining consent from users or making disclosures required under BIPA. The Court found that the plaintiff failed to allege sufficient contacts to show that Clarifai directly targeted Illinois and to establish personal jurisdiction.

ii. Illinois Bill Seeks to Limit BIPA

On March 22, the Illinois state legislature sent proposed amendments to BIPA (H.B. 559) to the chamber floor.[35] The draft bill contains provisions that would impose significant limitations on the scope and impact of BIPA, including a 30-day cure period, a one-year deadline to sue, and a proposal to replace statutory damages with actual damages.[36] BIPA suits have proliferated after the Illinois Supreme Court and some federal courts allowed plaintiffs to sue based on statutory violations.

D. FDA's Action Plan for AI Medical Devices

On January 12, 2021, the U.S. Food and Drug Administration ("FDA") released the agency's first "Artificial Intelligence/Machine Learning ("AI/ML")-Based Software as a Medical Device (SaMD) Action Plan," which describes a multi-pronged approach to advance the FDA's oversight of AI/ML-based medical software.[37] The AI/ML Action Plan is a response to stakeholder feedback received in relation to the April 2019 discussion paper, "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device (SaMD)," which described the foundation for a potential approach to premarket review for AI and ML software modifications.[38] For a detailed analysis of the discussion paper and proposed regulatory approach, please see our previous 2Q19 Legal Update.[39]

The FDA's "Action Plan" outlines five next steps:

1. Further developing the proposed regulatory framework, including through issuance of draft guidance on a predetermined change control plan (for software's learning over time). The SaMD Pre-Specifications ("SPS") describe "what" aspects the manufacturer intends to change through learning, and the Algorithm Change Protocol ("ACP") explains "how" the algorithm will learn and change while remaining safe and effective. The FDA intends to draft guidance which includes include a proposal of what should be included in an SPS and ACP to support the safety and effectiveness of AI/ML SaMD algorithms;
2. Supporting the development of good machine learning practices to evaluate and improve machine learning algorithms;
3. Fostering a patient-centered approach, including device transparency to users. Promoting transparency is a key aspect of a patient-centered approach, and numerous stakeholders have expressed the unique challenges of labeling for AI/ML-based devices and the need for manufacturers to clearly describe, for example, the data that were used to train the algorithm or "the role intended to be served by its output."[40] The FDA intends to identify types of information a manufacturer should include in the labeling of AI/ML based medical devices to support transparency to users.
4. Developing methods to evaluate and improve machine learning algorithms, which

includes methods for the identification and elimination of bias; and

5. Advancing real-world performance monitoring pilots on a voluntary basis.

The FDA welcomes continued feedback in this area and intends to hold public workshops to share learnings and elicit additional input from stakeholders. While the FDA has not yet expressed a substantive view on the specific contents of a draft regulation, it seems clear that it will involve a commitment from manufacturers on transparency and real-world performance monitoring for AI and machine learning-based software as a medical device, as well as periodic updates to the FDA on what changes were implemented as part of approved pre-specifications and the ACP. Depending on the scope of the draft regulatory framework, some of the proposed requirements could be highly significant and onerous: for example, requiring a manufacturer to include in the labeling of AI/ML-based devices a "description" of training data. We will continue to monitor developments, and expect that companies operating in this space will want to have a voice in the process leading up to the regulations, particularly with respect to implementing transparency requirements.

E. Intellectual Property Updates

1. *USPTO Files Motion for Summary Judgment Arguing that AI Machines Can't Invent*

On February 24, the U.S. Patent and Trademark Office ("USPTO") filed a motion for summary judgment in Virginia federal court with respect to a lawsuit challenging its finding that patents cannot cover inventions by AI machines, arguing that the Patent Act defines an inventor as an "individual" who must be human.[41]

The plaintiff, Stephen Thaler, is a physicist who created the AI, called DABUS, behind potential patents for a beverage container and a flashing beacon for search-and-rescue missions. The USPTO had denied the patent applications as incomplete because they were missing an inventor's name, and it refused a petition to reconsider in April 2020, noting that the courts and the law have made clear that only humans can be inventors. Thaler then sued the USPTO in August 2020, alleging it violated the Administrative Procedure Act when it added a patentability requirement that is "contrary to existing law and at odds with the policy underlying the patent system," and that by refusing to let AI machines be inventors, the agency is undermining the patent system.

In January 2021, Thaler filed a motion for summary judgment, arguing that the USPTO's finding was arbitrary, capricious, an abuse of discretion and not supported by the law or substantial evidence, and that all of the cases the USPTO cites to support its finding involve inventions that courts concluded humans could do, but not creations that only a machine could invent. At a motion hearing on April 6, U.S. District Judge Leonie Brinkema did not make a bench ruling, but indicated that current legislation restricts the definition of "inventor" in the Patent Act to humans.[42] As previously reported, the European Patent Office has also denied Thaler's patent applications with respect to DABUS.[43]

2. *Google LLC v. Oracle America, Inc*. — Supreme Court Rules for Google in Oracle Copyright Dispute

On April 5, the U.S. Supreme Court ruled in favor of Google in a multibillion-dollar copyright lawsuit filed by Oracle, holding that Google did not infringe Oracle's copyrights under the fair use doctrine when it used material from Oracle's API's to build its Android smartphone platform.[44] Notably, the Court did not rule on whether Oracle's API's declaring code could be copyrighted, but held that, assuming for argument's sake the material was copyrightable, "the copying here at issue nonetheless constituted a fair use."[45] Specifically, the Court stated that "where Google reimplemented a user interface, taking only what was needed to allow users to put their accrued talents to work in a new and transformative program, Google's copying of the Sun Java API was a fair use of that material as a matter of law."[46] The Court focused on Google's transformative

use of the Sun Java API and distinguished declaring code from other types of computer code in finding that all four guiding factors set forth in the Copyright Act's fair use provision weighed in favor of fair use.[47]

While the ruling appears to turn on this particular case, it will likely have repercussions for AI and platform creators.[48] The Court's application of fair use could offer an avenue for companies to argue for the copying of organizational labels without a license. Notably, the Court stated that commercial use does not necessarily tip the scales against fair use, particularly when the use of the copied material is transformative. This could assist companies looking to use content to train their algorithms at a lower cost, putting aside potential privacy considerations (such as under BIPA). Meanwhile, companies may also find it more challenging to govern and oversee competitive programs that use their API code for compatibility with their platforms.

F. U.S. Regulators Seek Input on AI Use in Financial Services

Five federal agencies, including the Federal Reserve Board and the Consumer Financial Protection Bureau, are seeking public input on financial institutions' use of AI. The notice "Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning" ("RFI") was published in the Federal Register on March 31.[49]

The federal agencies are aiming to better understand the use of AI and its governance, risk management and controls as well as challenges in developing, implementing and managing the technology. The RFI also solicits respondents' views on "the use of AI in financial services to assist in determining whether any clarifications from the agencies would be helpful for financial institutions' use of AI in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection." Financial institutions, trade associations, consumer groups and other stakeholders have until June 1, 2021 to submit their comments.

III. EU POLICY & REGULATORY DEVELOPMENTS

A. EC Publishes Draft Legislation for EU-wide AI Regulation

On April 21, 2021, the European Commission ("EC") presented its much anticipated comprehensive draft of an AI Regulation (also referred to as the "Artificial Intelligence Act").[50] As highlighted in our client alert "EU Proposal on Artificial Intelligence Regulation Released" and in our "3Q20 Artificial Intelligence and Automated Systems Legal Update", the draft comes on the heels of a variety of publications and policy efforts in the field of AI with the aim of placing the EU at the forefront of both AI regulation and innovation. The proposed Artificial Intelligence Act delivers on the EC president's promise to put forward legislation for a coordinated European approach on the human and ethical implications of AI[51] and would be applicable and binding in all 27 EU Member States.

In order to "achieve the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology"[52], the EC generally opts for a risk-based approach rather than a blanket technology ban. However, the Artificial Intelligence Act also contains outright prohibitions of certain "AI practices" and some very far-reaching provisions aimed at "high-risk AI systems", which are somewhat reminiscent of the regulatory approach under the EU's General Data Protection Regulation ("GDPR"); *i.e.* broad extra-territorial reach and hefty penalties, and will likely give rise to controversy and debate in the upcoming legislative procedure.

As the EC writes in its explanatory memorandum to the Artificial Intelligence Act, the proposed framework covers the following specific objectives:

- Ensuring that AI systems available in the EU are safe and respect EU laws and

values;

- Ensuring legal certainty to facilitate investment and innovation in AI;
- Enhancing governance and effective enforcement of existing laws applicable to AI (such as product safety legislation); and
- Facilitating the development of a single market for AI and prevent market fragmentation within the EU.

1. *Summary of Key Provisions*

The most relevant and noteworthy provisions contained in the Artificial Intelligence Act include:

1. *Scope of the Artificial Intelligence Act* – The proposed Artificial Intelligence Act not only covers "providers"[53] based in the EU, but also "providers" of AI systems based in third countries, placing on the market or putting into service AI systems in the EU, and also "users"[54] of AI systems located within the EU.[55] However, the proposed scope of the Artificial Intelligence Act goes even further to include also "providers" and "users" of AI systems located in third countries, where the output produced by the AI system is used in the EU.[56] The EC does not provide concrete examples for these use cases, but explains that the logic behind this is to prevent the circumvention of the Artificial Intelligence Act by transferring data lawfully collected in the EU to a third country and subject it to an AI system, which is located there.[57] Conversely, the Artificial Intelligence Act would not apply to AI systems developed or used exclusively for military purposes.[58]
2. *Definition of an AI system* – While the Artificial Intelligence Act provides a definition of an AI system[59], the EC emphasizes that the definition aims to be as technology neutral and future-proof as possible. Thus, the definition can and likely will be adapted by the EC as needed.
3. *Prohibition of certain AI practices* – Following a risk-based approach, which differentiates between uses of AI that create (i) an unacceptable risk, (ii) a high risk and (iii) low or minimal risk, the EC proposes to enact a strict ban on AI systems that are considered to create an "unacceptable risk." The Artificial Intelligence Act lists four types of AI systems bearing an unacceptable risk, including AI systems that deploy "subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm."[60] Since the draft legislation itself and the accompanying materials do not offer any further definitions or explanations for key terms, the exact application and impact of this prohibition in practice remains unclear. Further prohibited practices include the use of "social scoring" AI systems by public authorities[61] and the deployment of "real-time remote biometric identification systems" in publicly available spaces for the purpose of law enforcement (unless certain narrowly defined exceptions apply).[62]
4. *Mandatory requirements for "high-risk AI systems"* – The Artificial Intelligence Act contains specific requirements for so-called "high-risk AI systems". AI systems are considered "high-risk" if they are either (i) intended to be used as a safety component of a product (embedded AI) or are themselves a product, which is covered by certain EU product safety legislation (*g.* medical devices, personal protective equipment, toys or machinery)[63] or (ii) listed in an enumerative catalogue,[64] which may be expanded by the EC through the application of a specific risk assessment methodology. The latter includes, *inter alia*, biometric identification and categorization of natural persons, management and operation of critical infrastructure (*e.g.* supply of water, gas, heating and electricity), employment (*e.g.* AI systems for screening applications), access to and enjoyment of essential private services and public services and benefits (*e.g.* AI systems for evaluating credit scores), law enforcement (*e.g.* predictive AI systems intended for the evaluation of occurrence or reoccurrence of a criminal offence) and

administration of justice and democratic processes (*e.g.* AI systems for researching and interpreting facts and the law). Conspicuously, the health-care sector is missing from that list. General requirements for the development and deployment of such "high-risk AI systems" include the establishment and maintenance of a risk management system, the use of appropriate training, validation and testing data in the development phase, the achievement of an appropriate level of accuracy, robustness and cybersecurity in light of the intended use, the drawing up of specific technical documentation, designing of logging capabilities within the AI system, providing of comprehensive instructions for use and enabling human oversight of the AI system.[65] Notably, Article 10 of the draft regulation requires that the training, validation and testing data sets are "relevant, representative, free of errors and complete" and take into account the characteristics or elements particular to the specific geographical, behavioral or functional setting of the system's intended use; the draft regulation carves out higher penalties for non-compliance with these data and data governance requirements in comparison to other cases of infringement.[66] Providers of "high-risk AI systems" also have specific obligations, which include ensuring that high-risk AI systems undergo a "conformity assessment procedure" prior to placing on the market or putting into service.[67] This "conformity assessment procedure" is modelled after the procedures, which are required before introducing other products, such as medical devices, into the EU market. For certain "high-risk AI systems" the provider only needs to perform internal controls. However, for AI systems which enable biometric identification and categorization of natural persons, the providers must involve an outside entity in the assessment procedure (a so-called "notified body").[68] For "high-risk AI systems" covered by existing EU product safety legislation, already applicable conformity assessment procedures should be followed. Further, providers of "high-risk AI systems" must register the system in a publicly available EU database that is provided for under the Act.[69]

5. *Post-market monitoring obligations for "high-risk AI systems"* – In addition to the provisions relating to the development and placing on the market of "high-risk AI systems", the proposed Artificial Intelligence Act also provides for mandatory post-market monitoring obligations for providers of such systems.[70] This includes obligations to report any serious incident or any malfunctioning of the AI system, which would constitute a breach of obligations under EU laws intended to protect fundamental rights. "High-risk AI systems" also have to be withdrawn or recalled, if the provider considers that an AI system that was placed on the market or put into service violates the Artificial Intelligence Act.

6. *Provisions relating to "non-high-risk AI systems"* – Other AI systems which do not qualify as prohibited or "high-risk AI systems" are not subject to any specific requirements. In order to facilitate the development of "trustworthy AI", the EC stipulates that providers of "non-high-risk AI systems" should be encouraged to develop codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to "high-risk AI systems".[71] However, AI systems which are intended to interact with natural persons must be designed and developed in such a way that users are informed they are interacting with an AI system, unless it is "obvious from the circumstances and the context of use."[72] The EC also proposes a disclosure obligation for so-called "deep fakes".[73] In addition, the EC points out that such "non-high-risk AI systems" nevertheless have to comply with general product safety requirements.[74]

7. *Enforcement and penalties for non-compliance* – The draft Artificial Intelligence Act creates a governance and enforcement structure within which EU Member States would designate one or more national competent authorities at the national level, as well as a top-level national supervisory authority. At the EU level, the EC proposes establishing a European Artificial Intelligence Board, which would be responsible for providing advice and assistance to the EC. Finally, the proposal also includes various enforcement instruments and hefty penalties for non-compliance. In case of non-compliance with regards to the prohibitions on specific

AI systems under Article 5 and AI system requirements relating to data and data governance under Article 10, companies would face fines of up to EUR 30 million (approx. $36 million total global annual turnover, whichever is higher.[75] Cases of non-compliance with the remaining requirements and obligations under the draft regulation would subject the company to administrative fines of up to EUR 20 million (approx. $24 million) or up to 4% of the company's total worldwide annual turnover for the preceding financial year, whichever is higher.[76] Additionally, the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request may result in administrative fines of up to EUR 10 million (approx. $12 million) or up to 2% of the company's total worldwide annual turnover for the preceding financial year, whichever is higher.[77]

2. *Comparison with U.S. Legislative Proposals*

Although the draft EC regulation is more comprehensive than existing legal frameworks that govern AI, there are marked similarities to recent legislation introduced in the U.S. For example, as noted above, a growing number of legislative bodies in the U.S. have passed laws restricting or banning the use of facial recognition technology, sharing the EC's concerns regarding remote biometric identification systems, especially in the context of law enforcement.[78]

Additionally, like the draft regulation, state legislation relating to AI systems has called for increased transparency and stronger oversight. For example, the California Privacy Rights Act of 2020 requires that responses to access requests regarding automated decision-making technology "include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer", similar to the technical documentation requirements in the draft regulation which require providers to report "the general logic of the AI system and of the algorithms" along with the "main classification choices" with regards to the persons on which the system is to be used.[79] Also, like the supervising authority access requirements in the Artificial Intelligence Act, Washington state's "Act Relating to the use of facial recognition services", requires that providers of facial recognition services to state or local agencies "make available an application programming interface or other technical capability, chosen by the provider, to enable legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations."[80]

Notably, the transparency and technical documentation requirements in the EC's Artificial Intelligence Act are far more extensive than those outlined in existing legislation within the U.S. Specifically, under the EC regulation, authorities would be granted full access to the AI system provider's training, validation and testing datasets, and upon reasoned request, the source code itself.[81] While a court in New Jersey recently granted a criminal defendant access to the source code of a probabilistic genotyping software used to match the defendant's DNA to a crime scene, access to source code is generally not required by legislation or demanded by courts with respect to automated-decisions in the United States.[82] The extensive required disclosures may cause concern over intellectual property protection; information and data would be protected by confidentiality requirements, however the Commission and Member States are permitted to exchange confidential information with regulatory authorities of third countries where confidentiality agreements are in place.[83] Currently, United States legislative and regulatory bodies are not asking for the same degree of transparency, but are still taking steps to curb the potential discriminatory impact of AI systems, as discussed above.[84]

3. *Next Steps*

While it is uncertain when and in which form the Artificial Intelligence Act will come into force, the EC has set the tone for upcoming policy debates with this ambitious new proposal. While certain provisions and obligations may not be carried over to the final

legislation, it is worth noting that the EU Parliament has already urged the EC to prioritize ethical principles in its regulatory framework.[85] Therefore, we expect that the proposed rules will not be significantly diluted, and could even be further tightened, as some advocacy groups have called for.[86] Companies developing or using AI systems, whether based in the EU or abroad, should keep a close eye on further developments with regard to the Artificial Intelligence Act, and in particular the scope of the prohibited "unacceptable" and "high-risk" use cases, which, as drafted, could potentially apply to a very wide range of products and applications.

We stand ready to assist clients with navigating the potential issues raised by the proposed EU regulations as we continue to closely monitoring developments in that regard, as well as public reaction. We can and will help advise any clients desiring to have a voice in the process.

B. CAHAI Feasibility Study on AI Legal Standards

On December 17, 2020, the Ad Hoc Committee on Artificial Intelligence ("CAHAI") of the Council of Europe (the "CoE"), adopted a feasibility study on a legal framework on AI design, development and application based on the CoE's standards.[87] CAHAI was mandated by the CoE in 2019 to examine, on the basis of broad multi-stakeholder consultations, the feasibility of such a legal framework and take into account the CoE's relevant standards in the fields of human rights, democracy and the rule of law as well as the relevant existing universal and regional international legal instruments.

At the outset, CAHAI points out that there is no single definition of AI and that the term "AI" is used as a blanket term for "various computer applications based on different techniques, which exhibit capabilities commonly and currently associated with human intelligence." Accordingly, CAHAI highlights the need to approach AI systems in a technologically neutral way.

CAHAI expressly recognizes the opportunities and benefits arising from AI—such as contributing to achieving the UN Sustainable Development Goals and helping to mitigate the effect of climate change—but also addresses the potential challenges of certain AI use cases, such as the use of AI systems to predict recidivism and AI-based tracking techniques, as well as the risks arising out of biased training data. In light of these concerns, CAHAI recommends that a potential CoE legal framework on AI should pursue a risk-based approach that targets the specific application context. In its concluding comments, CAHAI notes that "no international legal instrument specifically tailored to the challenges posed by AI exists, and that there are gaps in the current level of protection provided by existing international and national instruments."

On March 30, 2021, the CoE announced that CAHAI is now preparing a legal framework on AI.[88] CAHAI has launched a multi-stakeholder consultation until April 29, 2021.[89]

C. EU Council Proposes ePrivacy Regulation

On February 10, 2021, the Council of the European Union (the "EU Council"), the institution representing EU Member States' governments, provided a negotiating mandate with regard to a revision of the ePrivacy Directive [90] and published an updated proposal for a new ePrivacy Regulation.[91] Contrary to the current ePrivacy Directive, the new ePrivacy Regulation would not have to be implemented into national law, but would apply directly in all EU Member States without transposition.

The ePrivacy Directive[92] contains rules related to the privacy and confidentiality in connection with the use of electronic communications services. However, an update of these rules is seen as critical given the sweeping and rapid technological advancement that has taken place since it was adopted in 2002. The new ePrivacy Regulation, which would repeal and replace the ePrivacy Directive, has been under discussion for several

years now.[93]

Pursuant to the EU Council's proposal, the ePrivacy Regulation will also cover machine-to-machine data transmitted via a public network, which might create restrictions on the use of data by companies developing AI-based products and other data-driven technologies. As a general rule, all electronic communications data will be considered confidential, except when processing or other usage is expressly permitted by the ePrivacy Regulation. Similar to the European General Data Protection Regulation ("GDPR"), the ePrivacy Regulation would also apply to processing that takes place outside of the EU and/or to service providers established outside the EU, provided that the end users of the electronic communications services, whose data is being processed, are located in the EU.

However, unlike GDPR, the ePrivacy Regulation would cover all communications content transmitted using publicly available electronic communications services and networks, and not only personal data. Further, metadata (such as location and time of receipt of the communication) also falls within the scope of the ePrivacy Regulation.

It is expected that the draft proposal will undergo further changes during negotiations with the European Parliament. Therefore, it remains to be seen whether the particular needs of highly innovative data-driven technologies will be taken into account—by creating clear and unambiguous legal grounds other than user consent for processing of communications content and metadata for the purpose of developing, improving and offering AI-based products and applications. If the negotiations between the EU Council and the EU Parliament proceed without any further delays, the new ePrivacy Regulation could enter into force in 2023, at the earliest.

D. Cybersecurity Report on the Use of AI in Autonomous Vehicles

On February 11, 2021, the European Union Agency for Cybersecurity ("ENISA") and the European Commission's Joint Research Centre ("JRC") published a joint report on cybersecurity risks connected to the use of AI in autonomous vehicles and provided recommendations for mitigating them (the "Cybersecurity Report").[94]

The Cybersecurity Report emphasized the vulnerability of AI systems in autonomous vehicles with respect to intentional attacks that aim to interfere with the AI system. Even simple measures, such as paint markings on the road, could interfere with system navigation tools using AI technologies and could have a significant impact on safety and reliability.

In order to prevent or mitigate such risks, the Cybersecurity Report recommends several measures, such as the systematic security validation of AI models and data early on in the development process of AI systems used in autonomous vehicles. Further, the automotive industry should adopt a holistic "security by design" approach, creating an "AI cybersecurity culture" across the production ecosystem. The Cybersecurity Report identifies the absence of sufficient security knowledge and expertise among developers and system designers as a major roadblock towards cybersecurity awareness in the industry.

E. Proposed German Legislation on Autonomous Driving

On March 15, 2021, the German Federal Government ("Bundesregierung") submitted a draft law on fully automated driving (SAE level 4) to the German Parliament ("Bundestag") for legislative debate.[95] The draft law aims to establish uniform conditions for testing new technologies, such as driverless cars with SAE level 4, throughout Germany. Pursuant to the draft law, autonomous vehicles will be permitted to drive in regular operation without a driver being physically present, limited—for now—to certain locally defined operating areas, for the time being. If the draft law is passed by the *Bundestag*, Germany expects to be the

first country in the world to permit fully automated vehicles in regular operation across the country by 2022 (subject to local operating areas to be defined by the respective German state authorities). As an example of fields of operation for such automated vehicles, the Bundesregierung mentions shuttle services, Hub2Hub and Dual-Mode-Vehicles, such as "automated valet parking." Currently, autonomous vehicles can only be operated in Germany with special permits granted by state authorities.

The draft law also includes framework provisions on liability, which reflect the status quo under German liability law: if a person is injured or an object damaged while operating a car, the motor insurance of the car's owner compensates for the damage. However, the draft law also introduces a new concept: "technical supervision," defined as the ability to deactivate the autonomous vehicle during operation and enable driving maneuvers for the autonomous vehicle. In principle, the owner of the car is responsible for "technical supervision," but can also entrust another person with the performance of these tasks. Nonetheless, the owner is still liable for any possible liability of the person entrusted with "technical supervision."

There remains disagreement within the Bundesregierung regarding the provisions on data protection contained in the draft law.[96] Open items will be discussed in the upcoming legislative procedure. The Bundesregierung is aiming to adopt the new law before the parliamentary summer break (and before the German Federal Elections in September 2021).[97]

---

[1] This Legal Update focuses on recent U.S. and EU regulatory efforts, but we note that there are numerous other examples of increasingly stringent worldwide regulation of algorithmic accountability and fairness. For example, on February 22, the UK Government published its response to the December 2020 Report by the House of Lords Select Committee on Artificial Intelligence, "AI in the UK: No Room for Complacency," discussed in more detail in our Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems. The House of Lords' report recommended action by the Government and called for it to "better coordinate its [AI] policy and the use of data and technology" on a national and local level, and "lead the way on making ethical AI a reality." In its response, the UK Government acknowledged that it is crucial to develop the public's understanding and trust in AI, stating that the National Data Strategy is actively ensuring members of the public become "responsible data citizens". Moreover, the Centre for Data Ethics and Innovation's ("CDEI") future role will include AI monitoring and testing potential interventions in the tech landscape.

[2] For more detail, see our Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems.

[3] The White House, Press Release (Archived), *The White House Launches the National Artificial Intelligence Initiative Office* (Jan. 12, 2021), available at https://trumpwhitehouse.archives.gov/briefings-statements/white-house-launches-national-artificial-intelligence-initiative-office/.

[4] The White House, *Memorandum on Restoring Trust in Government Through Scientific Integrity and Evidence-Based Policymaking* (Jan. 27, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/27/memorandum-on-restoring-trust-in-government-through-scientific-integrity-and-evidence-based-policymaking/.

[5] Government Executive, *New Task Force Will Conduct Sweeping Review of Scientific Integrity Policies* (March 30, 2021), available at https://www.govexec.com/management/2021/03/new-task-force-will-conduct-sweeping-review-scientific-integrity-policies/173020/.

[6] Letter from Deputy Director Jane Lubchenco and Deputy Director Alondra Nelson, OSTP to all federal agencies (March 29, 2021), available at https://int.nyt.com/data/documenttools/si-task-force-nomination-cover-letter-and-call-for-nominations-ostp/ecb33203eb5b175b/full.pdf.

[7] The White House, *Executive Order on the President's Council of Advisors on Science and Technology* (Jan. 27, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/27/executive-order-on-presidents-council-of-advisors-on-science-and-technology/.

[8] House Armed Services Committee*, Subcommittee on Cyber, Innovative Technologies, and Information Systems*, available at https://armedservices.house.gov/cyber-innovative-technologies-and-information-systems.

[9] House Armed Services Committee, *Subcommittee on Cyber, Innovative Technologies, and Information Systems and the House Committee on Oversight & Reform's Subcommittee on National Security Joint Hearing: "Final Recommendations of the National Security Commission on Artificial Intelligence*" (Mar. 12, 2021), available at https://armedservices.house.gov/hearings?ID=32A667CD-578C-4F65-9F4F-1E26EE8F389A.

[10] H.R. 5515, 115th Congress (2017-18).

[11] The National Security Commission on Artificial Intelligence, *Previous Reports*, available at https://www.nscai.gov/previous-reports/.

[12] NSCAI, *The Final Report* (March 1, 2021), available at https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[13] Some of these concerns echo prior actions by the USPTO. For example, the USPTO issued the 2019 Revised Patent-Eligibility Guidance, which reportedly resulted in a 44% decrease in uncertainty of patent examination subject matter. However, the guidance has not been broadly applied by courts and leads to mixed results. Additionally, the USPTO in October 2020 issued a report on Public Views on Artificial Intelligence and Intellectual Property Policy, observing that commentators "were nearly equally divided between the view that new intellectual property rights were necessary to address AI inventions and the belief that the current U.S. IP framework was adequate to address AI inventions." As discussed below, however, the USPTO continues to hold the view that an inventor to a patent must be a natural person.

[14] Securing the Information and Communications Technology and Services Supply Chain, 86 FR 4909 (Jan. 19, 2021), available at https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

[15] Securing the Information and Communications Technology and Services Supply Chain, U.S. Department of Commerce, 86 Fed. Reg. 4923 (Jan. 19, 2021) (hereinafter "Interim Final Rule").

[16] Interim Final Rule, § 7.1.

[17] Further, on February 3, Canada's Privacy Commissioners stated that Clearview AI's app—which has been used widely by law enforcement agencies across Canada—was "illegal" and akin to putting all of society "continually in a police lineup.") (Link to PIPEDA report)

[18] FTC, Business Blog, Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI* (April 19, 2021), available at https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

[19] FTC, *Protecting Consumer Privacy in a Time of Crisis*, Remarks of Acting Chairwoman Rebecca Kelly Slaughter, Future of Privacy Forum (Feb. 10, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1587283/fpf_opening_remarks_210_.pdf.

[20] FTC, *Using Artificial Intelligence and Algorithms* (April 8, 2020), available at https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.

[21] FTC, *Prepared Opening Statement of Commissioner Rohit Chopra*, U.S. Senate Committee on Commerce, Science, and Transportation Hearing on "Strengthening the Federal Trade Commission's Authority to Protect Consumers," (April 20, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1589172/final_chopra_opening_statement_for_senate_commerce_committee_20210420.pdf.

[22] While a recent Supreme Court ruling curtailed the FTC's ability to seek equitable monetary penalties such as restitution or disgorgement (*AMG Capital Management, LLC, et al. v. Federal Trade Commission*, No. 19-508 (U.S. April 22, 2021), Congress is considering legislation to remedy the decision. The House Energy and Commerce Committee has scheduled a hearing on whether the FTC needs new authority to seek consumer redress. *See further* Christopher Cole, *Supreme Court Rolls Back FTC Restitution Power*, Law360 (April 22, 2021), available at https://www.law360.com/articles/1377854.

[23] S. ___, 117th Congress (2021), available at https://www.wyden.senate.gov/imo/media/doc/The%20Fourth%20Amendment%20Is%20Not%20For%20Sale%20Act%20of%202021%20Bill%20Text.pdf.

[24] Statement of Sen. Ron Wyden (D-OR), The Fourth Amendment Is Not For Sale Act (April 21, 2021), available at https://www.wyden.senate.gov/imo/media/doc/The%20Fourth%20Amendment%20Is%20Not%20For%20Sale%20Act%20of%202021%20One%20Pager.pdf.

[25] *Id*.

[26] For more details, see our Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems.

[27] S.B. 5116, Reg. Session (2021-22).

[28] Monica Nickelsburg, *Washington state lawmakers seek to ban government from using discriminatory AI tech*, GeewWire (Feb. 13, 2021), available at https://www.geekwire.com/2021/washington-state-lawmakers-seek-ban-government-using-ai-tech-discriminates/.

[29] FTC, *In the Matter of Everalbum, Inc. and Paravision, Commission File No. 1923172* (Jan. 11, 2021), available at https://www.ftc.gov/enforcement/cases-proceedings/1923172/everalbum-inc-matter.

[30] FTC, Statement of Commissioner Rohit Chopra, *In the Matter of Everalbum and Paravision*, Commission File No. 1923172 (Jan. 8, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf.

[31] H.B. 2031, Reg. Session (2020-2021).

[32] For more details, see our Fourth Quarter and 2020 Annual Review of Artificial

Intelligence and Automated Systems.

[33] Order, *Steven Vance et al. v. Microsoft Corp.*, No. 2:20-cv-01082, (W.D. Wash. March 15, 2021,) 2021 WL 963485

[34] Order, *Stein et al. v. Clarifai Inc.*, No. 1:20-cv-01937, (N.D. Ill. March 16, 2021), 2021 WL 1020997

[35] H.B. 559, 102nd Gen. Assembly, available at https://www.ilga.gov/legislation/BillStatus.asp?DocNum=559&GAID=16&DocTypeID=HB&SessionID=110&GA=102.

[36] Lauraann Wood, Illinois Bill Seeks To File Down Biometric Law's Sharp Teeth, Law360 (March 22, 2021), available at https://www.law360.com/cybersecurity-privacy/articles/1367329/illinois-bill-seeks-to-file-down-biometric-law-s-sharp-teeth?nl_pk=4e5e4fee-ca5f-4d2e-90db-5680f7e17547&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

[37] U.S. Food & Drug Administration, News Release, *FDA Releases Artificial Intelligence/Machine Learning Action Plan* (Jan. 12, 2021), available at https://www.fda.gov/news-events/press-announcements/fda-releases-artificial-intelligencemachine-learning-action-plan.

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

[39] 2Q19 Artificial Intelligence and Autonomous Systems Legal Update, III.A. FDA Releases White Paper Outlining a Potential Regulatory Framework for Software as a Medical Device (SaMD) That Leverages AI.

[40] *Supra*, n.16 at 5.

[41] *Stephen Thaler v. Andrew Hirshfeld et al.*, No. 1:20-cv-00903 (E.D. Va. Feb. 24, 2021).

[42] Cara Salvatore, *Giving AI Inventorship Would Be A Bridge Too Far, Judge Says,* Law360 (April 6, 2021), available at https://www.law360.com/articles/1354993.

[43] For more detail, see our Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems.

[44] *Google LLC v. Oracle Am., Inc.*, No. 18-956, 2021 WL 1240906, (U.S. Apr. 5, 2021).

[45] *Id.*, at *3.

[46] *Id.* at *20.

[47] See *id.*

[48] Bill Donahue, *Supreme Court Rules For Google In Oracle Copyright Fight*, Law360 (April 5, 2021), available at https://www.law360.com/ip/articles/1336521.

[49] 86 Fed. Reg. 16837.

[50] EC, *Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence and amending certain Union Legislative Acts (Artificial Intelligence Act)*, COM(2021) 206 (April 21, 2021), *available at* https://digital

-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.

[51] Ursula von der Leyen, *A Union that strives for more: My agenda for Europe*, available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

[52] *Supra*, note 39, p. 1.

[53] "Providers" are defined as a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge (*see* Art. 3 no. 2 of the Artificial Intelligence Act).

[54] "Users" are defined as any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity (*see* Art. 3 no. 4 of the Artificial Intelligence Act).

[55] Certain obligations also apply to "importers" and "distributors".

[56] *See* Art. 2 para. 1 point (c) of the Artificial Intelligence Act.

[57] *See* Recital (11) of the Artificial Intelligence Act.

[58] *See* Art. 2 para. 3 of the Artificial Intelligence Act.

[59] "AI system" is defined as software that is developed with one or more of the techniques and approaches listed in an Annex (such as machine learning approaches incl. deep learning, logic- and knowledge-based approaches and statistical approaches) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environment the interact with (*see* Art. 3 no. 1 of the Artificial Intelligence Act).

[60] *See* Art. 5 para. 1 point (a) of the Artificial Intelligence Act.

[61] *See* Art. 5 para. 1 point (c) of the Artificial Intelligence Act.

[62] *See* Art. 5 para. 1 point (d) of the Artificial Intelligence Act.

[63] *See* Art. 6 para. 1 of the Artificial Intelligence Act.

[64] *See* Art. 6 para. 2 in connection with Annex III of the Artificial Intelligence Act.

[65] *See* Art. 8 et seqq. of the Artificial Intelligence Act.

[66] *See* Art. 10 and 71 of the Artificial Intelligence Act.

[67] See Art. 16 points (a) and (e) of the Artificial Intelligence Act.

[68] *See* Art. 43 of the Artificial Intelligence Act.

[69] *See* Art. 16 point (f), 51 and 60 of the Artificial Intelligence Act.

[70] *See* Art. 61 et seq. of the Artificial Intelligence Act.

[71] *See* Recital (81) and Art. 69 of the Artificial Intelligence Act.

[72] *See* Art. 52 para. 1 of the Artificial Intelligence Act.

[73] *See* Art. 52 para. 3 of the Artificial Intelligence Act.

[74] *See* Recital (82) of the Artificial Intelligence Act.

[75] *See* Art. 71 of the Artificial Intelligence Act.

[76] *See Id.*

[77] *See Id.*

[78] *See e.g.*, Portland Ordinance No. 190114, "Prohibit the use of Face Recognition Technologies by private entities in places of public accommodation in the City", effective Jan. 1, 2021 (banning private entities from using Face Recognition Technologies in Places of Public Accommodation within the boundaries of the City of Portland); 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). For more information, see our U.S. Cybersecurity and Data Privacy Outlook and Review – 2021 and Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems.

[79] *See* Art. 6 para. 1 in connection with Annex IV of the Artificial Intelligence Act; CPRA Section 14, adding Cal. Civ. Code § 1798.140(z). For more detail see our alert regarding "The Potential Impact of the Upcoming Voter Initiative, the California Privacy Rights Act".

[80] *See* Art. 64 of the Artificial Intelligence Act; An Act Relating to the use of facial recognition services, S.B. 6280, 66th Leg., Reg. Sess. (Wash. 2020), *available at* http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/Senate/6280-S.SL.pdf?q=20201214093740.

[81] *See* Art. 64 of the Artificial Intelligence Act.

[82] *See State v. Pickett*, No. A-4207-19T4, 2021 WL 357765, at *2 (N.J. Super. Ct. App. Div. Feb. 3, 2021); *see e.g., Houston Fed'n of Tchrs., Loc. 2415 v. Houston Indep. Sch. Dist.,* 251 F. Supp. 3d 1168, 1179 (S.D. Tex. 2017) (stating that "[w]hen a public agency adopts a policy of making high stakes employment decisions based on secret algorithms incompatible with minimum due process, the proper remedy is to overturn the policy, while leaving the trade secrets intact"); An Act Relating to the use of facial recognition services, S.B. 6280, 66th Leg., Reg. Sess. (Wash. 2020), *available at* http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/Senate/6280-S.SL.pdf?q=20201214093740 (stating that "[m]aking an application programming interface or other technical capability [to enable review] does not require providers to do so in a manner that would increase the risk of cyberattacks or to disclose proprietary data.").

[83] *See* Art. 70 of the Artificial Intelligence Act.

[84] *Supra* at I.C.

[85] 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. For more detail, see our "3Q20 Artificial Intelligence and Automated Systems Legal Update".

[86] The New York Times, *Europe Proposes Strict Rules for Artificial Intelligence* (April 21, 2021), available at https://www.nytimes.com/2021/04/16/business/artificial-intelligence-regulation.html.

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

[88] Press release, *Launch of the CAHAI Multi-stakeholder Consultation* (March 30, 2021), available at https://www.coe.int/en/web/artificial-intelligence/-/lauch-of-the-cahai-multi-stakeholder-consultation.

[89] The CAHAI consultation is accessible here: https://www.coe.int/en/web/artificial-intelligence/cahai-multi-stakeholder-consultation.

[90] Press release, *Confidentiality of electronic communications: Council agrees its position on ePrivacy rules* (Feb. 10, 2021), available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/.

[91] EU Council, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)* (Feb. 10, 2021), available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[92] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

[93] *See* EU Commission, *Proposal for a Regulation on Privacy and Electronic Communications* (Jan. 10, 2017), available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications.

[94] Press release, *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving* (Feb. 11, 2021), available at https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving. The Cybersecurity Report is available for download at https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving/.

[95] Draft law of the Bundesregierung, *Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren*, Drucksache 19/27439 (March 15, 2021), available at https://dip21.bundestag.de/dip21/btd/19/274/1927439.pdf.

[96] For example, it has been reported that the Federal Ministry of Justice has raised concerns in relation to the question whether data such as driving routes can be transmitted to the Federal Criminal Police Office (the German equivalent to the FBI) upon request.

[97] Bundesregierung, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Oliver Luksic, Frank Sitta, Bernd Reuther, weiterer Abgeordneter und der Fraktion der FDP*, Drucksache 19/24851 (Dec. 28, 2020), available at https://dip21.bundestag.de/dip21/btd/19/256/1925626.pdf.

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Michael Walther, Kai Gesing, Christopher Timura, Frances Waldmann, Selina Grün, Prachi Mistry,

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