GIBSON DUNN

January 15, 2020

ARTIFICIAL INTELLIGENCE AND AUTOMATED SYSTEMS LEGAL UPDATE (4Q19)

To Our Clients and Friends:

After a slow start to the year, global efforts to regulate artificial intelligence technologies ("AI") have gained real momentum. The 116th U.S. Congress saw a record number of bills related to AI in 2019—the Filter Bubble Transparency Act being the latest—and in the final quarter of 2019 the Trump administration continued to take tentative steps towards articulating a "light-touch" federal policy that balances safety and innovation, collaboration and protectionism, whilst being sufficiently technically detailed to allow federal agencies to consider their regulatory response. California continues to buck the national trend and has taken legislative action to prohibit, among other things, the use of facial recognition technology by law enforcement.

Meanwhile, the EU is preparing to deliver much-anticipated draft AI legislation in early 2020, but has, as we discuss below, already taken a firm stance in favor of regulation that is broad in scope, focused on ethics, individual rights and corporate accountability, and "horizontally" applicable across industries, rather than specific sectors—in other words, GDPR-style principles of governance that are in many respects diametrically opposed to U.S. federal policy, which eschews the EU's "regulate-first" approach.

As we will address in more detail in our forthcoming 2019 Annual Legal Review of Artificial Intelligence and Automated Systems, these fast-moving global developments will have a significant impact on companies developing or operating AI products in the EU.

Table of Contents

I. Key U.S. Legislative and Regulatory Developments

A. FILTER BUBBLE TRANSPARENCY ACT, S. 2763

On October 31, 2019 a bipartisan group of senators introduced the Filter Bubble Transparency Act, the first substantive federal bill aimed at regulating algorithmic control of content on internet platforms. If enacted, the bill would require large-scale internet platforms to provide greater transparency to consumers by providing clear notice on the use, and enabling consumers to opt out, of personalized content curated by "opaque" algorithms so that they can "engage with a platform without being manipulated by algorithms driven by user-specific data"[1] and "simply opt out of the filter bubble."[2] "Filter bubble" refers to a zone of potential manipulation that exists within algorithms that curate or rank content in internet platforms based on user-specific data, potentially creating digital "echo chambers."[3] Sen. John Thune, R-S.D., one of the bill's sponsors, explained that the bill is intended to facilitate "a better understanding of how internet platforms use artificial intelligence and opaque algorithms to make inferences from the reams of personal data at their fingertips that can be used to affect behavior and influence outcomes."[4]

The proposed legislation covers "any public-facing website, internet application, or mobile application," such as social network sites, video sharing services, search engines and content aggregation services[5], and generally would prohibit the use of opaque algorithms on platforms without those platforms having first provided notice in a "clear, conspicuous manner on the platform whenever the user interacts with an opaque algorithm for the first time." The term "opaque algorithm" is defined as "an algorithmic ranking system[6] that determines the order or manner that information is furnished to a user on a covered internet platform based, in whole or part, on user-specific data that was not expressly provided by the user to the platform" in order to interact with it.[7] Examples of "user-specific" data include the user's history of web searches and browsing, geographical locations, physical activity, device interaction, and financial transactions.[8] Conversely, data that was expressly provided to the platform by the user for the purpose of interacting with the platform—such as search terms, saved preferences, an explicitly entered geographical location or the user's social media profiles[9]—is considered "user-supplied."

Additionally, the bill requires that users be given the option to choose to view content based on "input-transparent algorithms," a purportedly generic algorithmic ranking system that "does not use the user-specific data of a user to determine the order or manner that information is furnished to such user on a covered platform,"[10] and be able to easily switch between the opaque and the input-transparent versions.[11] By way of example, Sen. Marsha Blackburn (R-TN), another co-sponsor of the bill, explained that "this legislation would give consumers the choice to decide whether they want to use the algorithm or view content in the order it was posted."[12] However, there is nothing in the bill that would require platforms to disclose the use of algorithms unless they are using hyper-personal "user-specific" data for customization, and even "input-transparent" algorithms using "user-supplied" data would not necessarily show content in chronological order. Nor would platforms be required to disclose any source

code or explain how the algorithms used work. As drafted, the bill's goals of providing transparency and protecting consumers from algorithmic manipulation by "opting out" of personalized content appear to be overstated, and lawmakers will need to grapple with the proposed definitions to clarify the scope of the bill's provisions.[13]

Much like the Algorithmic Accountability Act, discussed in more detail in our Artificial Intelligence and Autonomous Systems Legal Update (1Q19), the bill is squarely targeted at "Big Tech" platforms—it would not apply to platforms wholly owned, controlled and operated by a person that did not employ more than 500 employees in the past six months, averaged less than $50 million in annual gross receipts, and annually collects or processes personal data of less than a million individuals.[14] Violations of the Act would be enforced with civil penalties by the Federal Trade Commission ("FTC") but, unlike the Algorithmic Accountability Act, the bill does not grant state attorneys general the right to bring civil suits for violations, nor expressly state that its provisions do not preempt state laws.

We will continue to monitor the bill, which is co-sponsored by four members of the Senate Committee on Commerce, Science, and Transportation, as it makes its way through Congress.

B. NSCAI REPORT ON U.S. NATIONAL SECURITY

On November 4, 2019, the National Security Commission on Artificial Intelligence ("NSCAI") — which was tasked by Congress to research ways to advance the development of AI for national security and defense purposes — released a much-anticipated interim report specifying five key areas where it said U.S. policy can improve in order to transition AI from "a promising technological novelty into a mature technology integrated into core national security missions."[15] Eric Schmidt, the chairman of the commission and the former head of Google's parent company Alphabet, noted that the commission worked with a number of U.S. government departments and agencies including the intelligence community, academia and the private sector, as well as allied partners such as the United Kingdom, Japan, Canada and Australia. Across all five principles, NSCAI said that ethical and responsible development and deployment of AI is a top priority, and noted that it is still developing best practices for operationalizing AI technologies that are trustworthy, explainable, and free of unwanted bias.

The five lines of effort are: invest in research and development; apply the technology to national security missions; train and recruit AI talent; protect and build upon U.S. technology advantages; and marshal global cooperation on artificial intelligence issues.

The commission's preliminary conclusion is that the U.S. "is not translating broad national AI strengths and AI strategy statements into specific national security advantages."[16] Notably, the commission reported that federal R&D funding has not kept pace with the potential of AI technologies, noting that the requested fiscal year 2020 federal funding for core AI research outside of the defense sector grew by less than 2 percent from the estimated 2019 levels.[17] Further, it noted that AI is not realizing its potential to execute core national security missions because agencies are failing to embrace the technology as a result of "bureaucratic impediments and inertia."[18] NSCAI also criticized the shortage of AI talent in government agencies, specifically in the Department of Defense ("DoD"). It made workforce development recommendations to federal agencies, including undertaking more widespread

use of AI technologies, and improving training on basic AI principles.[19] The commission asserted that the U.S. has a global technological advantage in terms of AI implementation, but also warned that China is rapidly closing the gap.[20] NSCAI recommended export controls to protect AI hardware,[21] and preservation of an open research system with U.S. academia. Finally, the commission said the U.S. should lead creation of AI norms worldwide by fostering international collaboration and establishing a network of allies dedicated to AI data sharing, R&D coordination, capacity building, and talent exchanges.[22] The commission also notes that it is exploring possible avenues for "AI-related diplomatic discussions with rivals such as China and Russia" in areas such as AI safety in order to protect common interests, promote responsible research and innovation, and limit dangerous uses.[23]

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

C. U.S. IMPOSES EXPORT CONTROLS ON CHINESE AI COMPANIES

On October 7, 2019, BIS announced that it will add 28 Chinese governmental and commercial organizations to the Entity List for engaging in or enabling activities contrary to the foreign policy interests of the United States.[24] The regulation includes China's leading AI companies, including Sense Time, Megvii Technology, Yitu, and Dahua Technology. Companies are required to comply with the notice as of the effective date, although it includes a standard "savings clause" exempting items that are already en route as of October 9, 2019. The Secretary of Commerce stated that this action was in response to "the brutal suppression of ethnic minorities within China[.]"[25]

D. CALIFORNIA'S SWEEPING ATTEMPTS TO REGULATE AI

1. Two New California Laws Ban Certain Deepfake Videos

As we previously reported in our Artificial Intelligence and Autonomous Systems Legal Update (3Q19), in the wake of a June 2019 hearing by the House Permanent Select Committee on Intelligence on the national security challenges of artificial intelligence, manipulated media, and deepfake technology, both the House and the Senate introduced legislation to regulate deepfakes. While those bills remains pending, California has taken action to restrict the specific use of deepfakes to influence elections and non-consensual pornographic deepfakes. On October 3, 2019 California's Gov. Newsom signed a bill (A.B. 730) banning anyone "from distributing with actual malice materially deceptive audio or visual media of the candidate" within 60 days of an election with the intent to injure the candidate's reputation or deceive a voter into voting for or against the candidate.[26] This measure exempts print and online media and websites if that entity clearly discloses that the deepfake video or audio file is inaccurate or of questionable authenticity. On October 3, Gov. Newsom also signed a bill (A.B. 602) banning pornographic deepfakes made without consent of the person depicted, creating a private right of action.[27] The law excepts "[c]ommentary, criticism, or disclosure that is otherwise protected by the California Constitution or the United States Constitution."

It will remain to be seen whether these laws will be challenged and whether they will pass Constitutional muster. Regardless, the use and proliferation of deepfakes will likely face greater legal and regulatory

scrutiny at both federal and state level going forward, and may impact technology platforms which permit users to upload, share or link content.

2. California Limits Police Body Camera Facial Recognition Technology

On October 8, Gov. Newsom signed bill A.B. 1215,[28] which places a three-year moratorium on any facial recognition technology used in police body cameras beginning January 1, 2020. This development follows San Francisco and Oakland bans on police use of facial recognition technology, as reported in our Artificial Intelligence and Autonomous Systems Legal Update (2Q19). The language of A.B. 1215 states that using biometric surveillance violates constitutional rights because it is the "functional equivalent" of requiring people to carry identification at all times.[29] The new law further regulates the collection of personal information, sounds in California's concern for overly broad collection of information, and may influence modifications to the California Consumer Privacy Act 2018 ("CCPA") regarding facial recognition (such as A.B. 1281, which would require businesses to give conspicuous notices where facial recognition technology is employed).

3. California AG Releases New California Consumer Privacy Act (CCPA) Proposed Regulations

As reported in our client alert California Consumer Privacy Act: 2019 Final Amendments Signed, on October 10, California Attorney General Xavier Becerra issued new draft regulations operationalizing the California Consumer Privacy Act ("CCPA"). The CCPA has been described as one of the most stringent state privacy laws and will affect AI technologies that are driven by personal data. We have previously published a summary of the CCPA as well as its initial amendments, and stand ready to advise companies who utilize or develop such technologies on the potential implications of CCPA within the AI space.

E. EC PROMISES "GDPR"-STYLE REGULATION OF AI

As reported in our Artificial Intelligence and Autonomous Systems Legal Update (3Q19), European Commission President Ursula von der Leyen promised to propose legislation to address the human and ethical implications of AI in the first quarter of 2020.[30] In a speech at the European Parliament on November 27, 2019, von der Leyen said that she was in favor of AI-focused legislation similar to the General Data Protection Regulation ("GDPR").[31] The Commission is likely to draw on the work of its high-level expert group on AI, which outlined a series of principles earlier this year aimed at ensuring companies deploy artificial intelligence in a way that is fair, safe and accountable.[32] The principles, developed by a committee of academics and industry representatives, form part of the EU's plan to increase public and private investment in AI to €20 billion per year.

We will monitor any further statements by the EC and provide updates on any proposed legislation as it becomes available. As we previously addressed in more detail in "Gearing Up for the EU's Next Regulatory Push: AI,"[33] given the stringent requirements of the GDPR, future EC regulations are likely to stand in contrast to the current U.S. "light-touch" regulatory approach and could have a significant impact on companies developing or operating AI products within the EU.

II. Bias/Ethics and Technology Bans

A. GERMAN DATA ETHICS COMMISSION REPORT

On October 23, 2019, Germany's Data Ethics Commission released a landmark 240-page report containing 75 recommendations for regulating data, algorithmic systems and AI.[34] Consistent with EC President Ursula von der Leyen's recent remarks discussed above, the report suggests that EU regulation of AI may mirror the approach espoused in the GDPR — broad in scope, focused on individual rights and corporate accountability, and "horizontally" applicable across industries, rather than specific sectors.[35] Expanding on the EU's non-binding "Ethics Guidelines for Trustworthy AI," the commission concludes that "regulation is necessary, and cannot be replaced by ethical principles."[36]

The commission creates a blueprint for the implementation of binding legal rules for AI—nominally both at national and EU level—on a sliding scale based on the risk of harm across five levels of algorithmic systems, with a focus on the degree of potential harm rather than differentiating between specific use cases. While systems posing a negligible or low likelihood of harm would not require any new regulatory obligations, those with at least "some" potential for harm would be subject to a mandatory labeling scheme that indicates where and how algorithms are being used within the system, and a risk assessment that evaluates the system's effect on privacy rights, self-determination, bodily or personal integrity, assets and ownership rights, and discrimination, among other factors. For systems that curate content based on user data, such as personalized pricing algorithms, the commission recommends prior authorization by supervisory institutions, and heightened oversight (such as live monitoring) and transparency obligations systems with "regular or significant potential for harm," which include determinations about consumer creditworthiness. The commission recommended a full or partial ban on systems with an "untenable potential for harm."[37]

Of particular relevance to companies deploying AI software, the report recommends that measures be taken against "ethically indefensible uses of data," such as "total surveillance, profiling that poses a threat to personal integrity, the targeted exploitation of vulnerabilities, addictive designs and dark patterns, methods of influencing political elections that are incompatible with the principle of democracy, vendor lock-in and systematic consumer detriment, and many practices that involve trading in personal data."[38]

The commission also recommends that human operators of algorithmic systems be held vicariously liable for any harm caused by autonomous technology, and calls for an overhaul of existing product liability and strict liability laws as they pertain to algorithmic products and services.[39]

While the report's pro-regulation approach is a counterweight to the "light-touch' regulation favored by the U.S. government, the commission takes the view that, far from impeding private sector innovation, regulation can provide much-needed certainty to companies developing, testing, and deploying innovative AI products.[40] Certainly, the commission's guiding principles—among them the need to ensure "the human-centred and value-oriented design of technology"[41]—reinforce that European lawmakers are likely to regulate AI development comprehensively and decisively. While it remains to be seen to what extent the forthcoming draft EU legislation will adopt the commission's

recommendations, all signs point to a sweeping regulatory regime that could significantly impact technology companies active in the EU.

B. NEW DOD ETHICS FRAMEWORK

On October 31, 2019, the Defense Innovation Board ("DIB"), an independent federal advisory committee to the Pentagon consisting of a group of science and technology experts led by former Google CEO Eric Schmidt, proposed a new ethics framework consisting of five overarching ethical principles which tie the Department of Defense's ("DOD") existing laws of war and rules of engagement[42] into the use of AI.[43]

The report is a high-level blueprint for military deployments of artificial intelligence and addresses some general shortcomings of AI technology.[44] The principles advocate for deliberate AI designs to counter unintended biases that could cause inadvertent harm and for humans to have the power to deactivate or disengage AI systems acting outside the intended parameters. The board also suggested that humans should always be responsible for the "development, deployment, use and outcomes" of AI rather than letting AI set its own standards of use: "Governability is important because operators and users of AI systems should understand the potential consequences of deploying the system or system of systems to its full extent, which may lead to unintended harmful outcomes." In these cases, DOD should not use that AI system because "it does not achieve mission objectives in an ethical or responsible manner."[45]

The DIB also recommended a number of technical and organizational measures that would help lay the groundwork to ensure military artificial intelligence systems adhere to ethical standards, such as increasing investment in standards development, workforce programs and AI security applications, and formalizing channels for exploring the ethical implications of deploying AI technology across the department.

The report follows concerns that most AI-related innovation is being developed by commercial technology firms rather than its internal research or traditional industrial base, and that some firms are reluctant to take on defense contracts at least in part due to ethical conflicts.[46] The newly proposed ethics framework could help address private sector concerns about innovative technology being wrongly weaponized or misused by the military or being part of autonomous systems without sufficient human oversight. However, the report's recommendations are not binding, and Pentagon leaders will need to decide whether to enact the board's recommendations into concrete policy going forward.

III. Intellectual Property Law

A. USPTO REQUEST FOR COMMENT

Intellectual property issues related to AI have also been at the forefront of the new technology, as record numbers of U.S. patent applications involve a form of machine learning component. As we reported previously in our Artificial Intelligence and Autonomous Systems Legal Update (4Q18), 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.[47] The request for comment posed twelve questions covering several topics from "patent examination policy to whether new forms of intellectual property protection are needed." The questions included topics such whether patent laws, which contemplate only human inventors, should be amended to allow entities other than a human being to be considered an inventor.[48] The commenting period was extended until November 8, 2019, and many of the comments submitted argue that ownership of patent rights should remain reserved for only natural or juridical persons.[49]

On December 13, 2019, the World Intellectual Property Organization ("WIPO") published a draft issue paper on IP policy and AI, and requested comments on several areas of IP, including patents and data, and, similarly to the USPTO before it, with regard to issues of inventorship and ownership.[50] The commenting period is set to end on February 14, 2020.

---

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

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

[3] *Supra*, n.2; *see also* Zoe Schiffer, *'Filter Bubble' author Eli Pariser on why we need publicly owned social networks*, The Verge (Nov. 12, 2019), available at https://www.theverge.com/2019/11/5/20943634/senate-filter-bubble-transparency-act-algorithm-personalization-targeting-bill.

[4] Colleagues Introduce Bipartisan Bill to Increase Internet Platform Transparency and Provide Consumers With Greater Control Over Digital Content, John Thune U.S. Senator for South Dakota (Nov. 1, 2019), https://www.thune.senate.gov/public/index.cfm/press-releases?ID=E1595915-69A3-456B-8CBA-0237F28AB4A3.

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

[6] *Id*. at 2(B). The term "algorithmic ranking system" is broadly defined and encompasses any computational process — including "one derived from algorithmic decision-making, machine learning, statistical analysis, or other data processing or artificial intelligence techniques" — that is used to determine the order in which a set of information is provided to a user on a covered internet platform.

Examples include "the ranking of search results, the provision of content recommendations, the display of social media posts, or any other method of automated content selection."

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

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

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

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

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

[12] *Supra*, n.2.

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

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

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

[16] *Id*., at 22.

[17] *Id*., at 25.

[18] *Id*., at 31.

[19] *Id*., at 36.

[20] *Id*., at 18.

[21] *Id*., at 41. Note that the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") announced on October 7, 2019 that it will be imposing new export controls on the export of U.S.-origin software specially designed to automate the analysis of geospatial imagery. A license from BIS will be required to export the covered software to all countries, except Canada, or to transfer the software to foreign nationals. The only exception to this license requirement is for software transferred by or to a department or agency of the U.S. Government.

[22] *Id*., at 44.

[23] *Id*.

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

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

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

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

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

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

[30] Ursula von der Leyen, *A Union that strives for more: My agenda for Europe*, available at https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf/.

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

[32] For more information, please see our Artificial Intelligence and Autonomous Systems Legal Update (1Q19).

[33] 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.

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

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

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

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

[38] *Id*., at 10.

[39] *Id*., at 26.

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

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

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

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

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

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

[46] *Id*.

[47] 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.

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

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

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

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Frances Waldmann and Claudia Barrett.

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)
Lisa A. Fontenot - Palo Alto (+1 650-849-5327, lfontenot@gibsondunn.com)
David H. Kennedy - Palo Alto (+1 650-849-5304, dkennedy@gibsondunn.com)
Ari Lanin - Los Angeles (+1 310-552-8581, alanin@gibsondunn.com)
Robson Lee - Singapore (+65 6507 3684, rlee@gibsondunn.com)
Carrie M. LeRoy - Palo Alto (+1 650-849-5337, cleroy@gibsondunn.com)
Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33 180, mwalther@gibsondunn.com)