GIBSON DUNN

2021 Artificial Intelligence and Automated Systems Annual Legal Review

Client Alert | January 20, 2022

Click for PDF

2021 was a busy year for policy proposals and lawmaking related to artificial intelligence ("AI") and automated technologies. The OECD identified 700 AI policy initiatives in 60 countries, and many domestic legal frameworks are taking shape. With the new Artificial Intelligence Act, which is expected to be finalized in 2022, it is likely that high-risk AI systems will be explicitly and comprehensively regulated in the EU. While there have been various AI legislative proposals introduced in Congress, the United States has not embraced a comprehensive approach to AI regulation as proposed by the European Commission, instead focusing on defense and infrastructure investment to harness the growth of AI.

Nonetheless —mirroring recent developments in data privacy laws—there are some tentative signs of convergence in US and European policymaking, emphasizing a risk-based approach to regulation and a growing focus on ethics and "trustworthy" AI, as well as enforcement avenues for consumers. In the U.S., President Biden's administration announced the development of an "AI bill of rights." Moreover, the U.S. Federal Trade Commission ("FTC") has signaled a particular zeal in regulating consumer products and services involving automated technologies and large data volumes, and appears poised to ramp up both rulemaking and enforcement activity in the coming year. Additionally, the new California Privacy Protection Agency will likely be charged with issuing regulations governing AI by 2023, which can be expected to have far-reaching impact. Finally, governance principles and technical standards for ensuring trustworthy AI and ML are beginning to emerge, although it remains to be seen to what extent global regulators will reach consensus on key benchmarks across national borders.

Related People

Tony Bedel

Brendan Krimsky

Samantha Abrams-Widdicombe

Leon S. Freyermuth

Frances Waldmann

I. U.S. NATIONAL POLICY, LEGISLATIVE EFFORTS, & ENFORCEMENT

A. U.S. National Policy

1. National AI Strategy

Almost three years after President Trump issued an Executive Order "Maintaining American Leadership in Artificial Intelligence" to launch the "American AI Initiative" and seek to accelerate AI development and regulation with the goal of securing the United States' place as a global leader in AI technologies, we have seen a significant increase in AI-related legislative and policy measures in the U.S., bridging the old and new administrations. As was true a year ago, the U.S. federal government has been active in

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

coordinating cross-agency leadership and encouraging the continued research and development of AI technologies for government use. To that end, a number of key legislative and executive actions have been directed at increasing the growth and development of such technologies for federal agency, national security and military applications. U.S. lawmakers also continued a dialogue with their EU counterparts, pledging to work together during an EU parliamentary hearing on March 1.[1] Rep. Robin Kelly (D-Ill.) testified at a hearing before the EU's Special Committee on AI, noting that "[n]ations that do not share our commitment to democratic values are racing to be the leaders in AI and set the rules for the world," .[2] She urged Europe to take a "narrow and flexible" approach to regulation while working with the U.S.[3]

a) National AI Initiative Act of 2020 (part of the National Defense Authorization Act of 2021 ("NDAA")) and National AI Initiative Office

Pursuant to the National AI Initiative Act of 2020, which was passed on January 1, 2021 as part of the National Defense Authorization Act of 2021 ("NDAA"),[4] the 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.[5] The Act also established the National AI Research Resource Task Force (the "Task Force"), convening a group of technical experts across academia, government and industry to assess and provide recommendations on the feasibility and advisability of establishing a National AI Research Resource ("NAIRR").[6] The Task Force will develop a coordinated roadmap and implementation plan for establishing and sustaining a NAIRR, a national research cloud to provide researchers with access to computational resources, high-quality data sets, educational tools and user support to facilitate opportunities for AI research and development. The Task Force will submit two reports to Congress to present its findings, conclusions and recommendations—an interim report in May 2022 and a final report in November 2022.

On January 27, 2021, 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[7] which is expected to "generate important insights and best practices including transparency and accountability…."[8] The President also signed an executive order to formally reconstitute the President's Council of Advisors on Science and Technology,[9] and announced the establishment of the National AI Advisory Committee, which is tasked with providing recommendations on various topics related to AI, including the current state of U.S. economic competitiveness and leadership, research and development, and commercial application.[10]

b) Innovation and Competition Act (S. 1260)

On June 8, 2021, the U.S. Senate voted 68-32 to approve the U.S. Innovation and Competition Act (S. 1260), intended to boost the country's ability to compete with Chinese technology by investing more than $200 billion into U.S. scientific and technological innovation over the next five years, listing artificial intelligence, machine learning, and autonomy as "key technology focus areas."[11] $80 billion is earmarked for research into AI, robotics, and biotechnology. Among various other programs and activities, the bill establishes a Directorate for Technology and Innovation in the National Science Foundation ("NSF") and bolsters scientific research, development pipelines, creates grants, and aims to foster agreements between private companies and research universities to encourage technological breakthroughs.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

The Act also includes provisions labelled as the "Advancing American AI Act,"[12] intended to "encourage agency artificial intelligence-related programs and initiatives that enhance the competitiveness of the United States" while ensuring AI deployment "align[s] with the values of the United States, including the protection of privacy, civil rights, and civil liberties."[13] The AI-specific provisions mandate that the Director of the Office for Management and Budget ("OMB") shall develop principles and policies for the use of AI in government, taking into consideration the NSCAI report, the December 3, 2020 Executive Order "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," and the input of various interagency councils and experts.[14]

c) Algorithmic Governance

We have also seen new initiatives taking shape at the federal level focused on algorithmic governance, culminating in the White House Office of Science and Technology Policy's ("OSTP") announcement in November 10, 2021, that it would launch a series of listening sessions and events the following week to engage the American public in the process of developing a Bill of Rights for an Automated Society.[15] According to OSTP Director Eric, the bill will need "teeth" in the form of procurement enforcement.[16] In a parallel action, the Director of the National AI Initiative Office, Lynne Parker made comments indicating that the United States should have a vision for the regulation of AI similar to the EU's General Data Protection Regulation ("GDPR").[17] Moreover, in October 2021, the White House's Office of Science and Technology Policy ("OSTP") published an RFI requesting feedback on how biometric technologies have performed in organizations and how they affect individuals emotionally and mentally.[18]

In June 2021, the U.S. Government Accountability Office ("GAO") published a report identifying key practices to help ensure accountability and responsible AI use by federal agencies and other entities involved in the design, development, deployment, and continuous monitoring of AI systems.[19] The report identified four key focus areas: (1) organization and algorithmic governance; (2) system performance; (3) documenting and analyzing the data used to develop and operate an AI system; and (4) continuous monitoring and assessment of the system to ensure reliability and relevance over time.[20]

Finally, the National Institute of Standards and Technology ("NIST"), tasked by the Trump administration to develop standards and measures for AI, released its report of how to measure and enhance user trust, and identify and manage biases, in AI technology.**[21]** NIST received sixty-five comments on the document, and the authors plan to synthesize and use the public's responses to develop the next version of the report and to help shape the agenda of several collaborative virtual events NIST will hold in coming months.**[22]**

2. National Security

a) 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."[23] 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.[24]

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

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

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[25] and identifies 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. These recommendations may have significant implications for potential oversight and regulation of AI in the private sector. The report also 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.

b) DOD's Defense Innovation Unit (DIU) released its "Responsible AI Guidelines"

On November 14, 2021, the Department of Defense's Defense Innovation Unit ("DIU") released "Responsible AI Guidelines" that provide step-by-step guidance for third party developers to use when building AI for military use. These guidelines include procedures for identifying who might use the technology, who might be harmed by it, what those harms might be, and how they might be avoided—both before the system is built and once it is up and running.[26]

c) Artificial Intelligence Capabilities and Transparency ("AICT") Act

On May 19, 2021, Senators Rob Portman (R-OH) and Martin Heinrich (D-NM), introduced the bipartisan Artificial Intelligence Capabilities and Transparency ("AICT") Act.[27] AICT would provide increased transparency for the government's AI systems, and is based primarily on recommendations promulgated by the National Security Commission on AI ("NSCAI") in April 2021.[28] AICT was accompanied by the Artificial Intelligence for the Military (AIM) Act.[29] The AICT Act would establish a pilot AI development and prototyping fund within the Department of Defense aimed at developing AI-enabled technologies for the military's operational needs, and would develop a resourcing plan for the DOD to enable development, testing, fielding, and updating of AI-powered applications.[30] Both bills were passed as part of the Fiscal Year 2022 National Defense Authorization Act.[31]

B. Consumer Protection, Privacy & Algorithmic Fairness

1. FTC Focuses on Algorithmic Transparency and Fairness

On April 19, 2021, the FTC issued guidance highlighting its intention to enforce principles of transparency and fairness with respect to algorithmic decision-making impacting consumers. The blog post, "Aiming for truth, fairness, and equity in your company's use of AI," announced the FTC'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.[32] 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 blog post provided 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 their algorithms for improper bias before and during deployment; employing transparency frameworks and independent standards; and being transparent

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

with consumers and seeking appropriate consent to use consumer data. The guidance also warned 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 came on the heels of remarks by former 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.[33] It also follows the FTC's informal guidance last year outlining principles and best practices surrounding transparency, explainability, bias, and robust data models.[34]

These regulatory priorities continue to gather pace under new FTC Chair Lina Khan, who in November 2021 announced several new additions to the FTC's Office of Policy Planning, including three "Advisors on Artificial Intelligence," Meredith Whittaker, Ambak Kak, and Sarah Meyers West—all formerly at NYU's AI Now Institute and experts in various AI topics including algorithmic accountability and the political economy of AI.[35]

The FTC has also taken steps to strengthen its enforcement powers, passing a series of measures to allow for quicker investigations into potential violations, including issues regarding bias in algorithms and biometrics.[36] Moreover, on July 27, 2021, the FTC's chief technologist Erie Meyer commented that the agency envisions requiring companies that engage in illegal data uses to "not just disgorge data and money," but also "algorithms that were juiced by ill-gotten data."[37] Sen. Mike Lee, R-Utah, subsequently introduced a bill on December 15, 2021 that would give the FTC the authority to seek restitution in federal district court, after the U.S. Supreme Court ruled in April that the agency's power to seek injunctions from a federal judge does not include the ability to request restitution or disgorgement of ill-gotten gains.[38] The proposed Consumer Protection and Due Process Act would amend Section 13(b) of the Federal Trade Commission Act to give the FTC the explicit authority to ask a federal judge to let it recover money from scammers and antitrust violators.[39]

The FTC also identified "dark patterns" as a growing concern and enforcement focal point. Dark patterns may be loosely defined as techniques to manipulate a consumer into taking an unintended course of action using novel uses of technology (including AI), particularly user experience (UX) design—for example, a customer service bot, unwanted warranty, or a trial subscription that converts to paid.[40] At an FTC virtual workshop to examine dark patterns, the Acting Director of the Bureau of Consumer Protection, Daniel Kaufman, suggested that companies can expect aggressive FTC enforcement in this area and that the FTC will use Section 5 of the FTC Act and the Restoring Online Shoppers' Confidence Act to exercise its authority by enacting new rules, policy statements, or enforcement guidance.[41]

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 and impose obligations to delete algorithms, models or data.

2. Consumer Financial Protection Bureau

The CFPB, now headed by former FTC Commissioner Rohit Chopra, suggested that it may use the Fair Credit Reporting Act (FCRA) to exercise jurisdiction over large technology companies and their business practices.[42] The FCRA has traditionally regulated the activities of credit bureaus, background check companies, and tenant screening services, but Chopra has made several statements that the underlying data

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

used by technology giants may be triggering obligations under the FCRA. The FCRA defines a consumer reporting agency fairly broadly to include companies assembling, evaluating, and selling data to third parties that use the data in making eligibility decisions about consumers. The CFPB may seek to make an inquiry into large technology companies in order to learn whether data is, in fact, being sold to third parties and how it may be used further downstream.

In November, the CFPB issued an advisory opinion affirming that consumer reporting companies, including tenant and employment screening companies, are violating the law if they engage in careless name-matching procedures.[43] The CFPB is particularly concerned by the algorithms of background screening companies assigning a false identity to applicants for jobs and housing due to error-ridden background screening reports that may disproportionately impact communities of color. The advisory opinion reaffirms the obligations and requirements of consumer reporting companies to use reasonable procedures to ensure the maximum possible accuracy.

3. U.S. Equal Employment Opportunity Commission

The U.S. Equal Employment Opportunity Commission plans to review how AI tools and technology are being applied to employment decisions.[44] The EEOC's initiative will examine more closely how technology is fundamentally changing the way employment decisions are made. It aims to guide applicants, employees, employers, and technology vendors in ensuring that these technologies are used fairly, consistent with federal equal employment opportunity laws.

4. Facial Recognition and Biometric Technologies

a) Enforcement

In January 2021, the 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.[45] 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.[46] We will carefully monitor any further enforcement action by the FTC (and other regulators), as well as the slate of pending lawsuits alleging the illicit collection of biometric data used by automated technologies pursuant to a growing number of state privacy laws—such as Illinois' Biometric Information Privacy Act ("BIPA")[47]—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 develop robust AI diligence and risk-assessment processes for third-party AI applications.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

b) Legislation

Facial recognition technology also attracted renewed attention from federal and state lawmakers in 2021. On June 15, 2021, a group of Democratic senators reintroduced the Facial Recognition and Biometric Technology Moratorium Act, which would prohibit agencies from using facial recognition technology and other biometric tech—including voice recognition, gate recognition, and recognition of other immutable physical characteristics—by federal entities, and block federal funds for biometric surveillance systems.[48] A similar bill was introduced in both houses in the previous Congress but did not progress out of committee.[49] The legislation, which is endorsed by the ACLU and numerous other civil rights organizations, also provides a private right of action for individuals whose biometric data is used in violation of the Act (enforced by state Attorneys General), and seeks to limit local entities' use of biometric technologies by tying receipt of federal grant funding to localized bans on biometric technology. Any biometric data collected in violation of the bill's provisions would also be banned from use in judicial proceedings.

At the state level, Virginia passed a ban on the use of facial recognition technology by law enforcement (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.[50] The law took 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.[51]

5. Algorithmic Accountability

a) Algorithmic Justice and Online Platform Transparency Act of 2021 (S. 1896)

On May 27, 2021, Senator Edward J. Markey (D-Mass.) and Congresswoman Doris Matsui (CA-06) introduced the Algorithmic Justice and Online Platform Transparency Act of 2021 to prohibit harmful algorithms, increase transparency into websites' content amplification and moderation practices, and commission a cross-government investigation into discriminatory algorithmic processes across the national economy.[52] The Act would prohibit algorithmic processes on online platforms that discriminate on the basis of race, age, gender, ability, and other protected characteristics. In addition, it would establish a safety and effectiveness standard for algorithms and require online platforms to describe algorithmic processes in plain language to users and maintain detailed records of these processes for review by the FTC.

b) Consumer Safety Technology Act, or AI for Consumer Product Safety Act (H.R. 3723)

On June 22, 2021, the House voted 325-103 to approve the Consumer Safety Technology Act, or AI for Consumer Product Safety Act (H.R. 3723), which requires the Consumer Product Safety Commission to create a pilot program that uses AI to explore consumer safety questions such as injury trends, product hazards, recalled products, or products that should not be imported into the U.S.[53] This is the second time the Consumer Safety Technology Act has passed the House. Last year, after clearing the House, the bill did not progress in the Senate after being referred to the Committee on Commerce, Science and Transportation.[54]

c) Data Protection Act of 2021 (S. 2134)

In June 2021, Senator Kirsten Gillibrand (D-NY) introduced the Data Protection Act of

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

2021, which would create an independent federal agency to protect consumer data and privacy.[55] The main focus of the agency would be to protect individuals' privacy related to the collection, use, and processing of personal data.[56] The bill defines "automated decisions system" as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision, or facilitates human decision making."[57] Moreover, using "automated decision system processing" is a "high-risk data practice" requiring an impact evaluation after deployment and a risk assessment on the system's development and design, including a detailed description of the practice including design, methodology, training data, and purpose, as well as any disparate impacts and privacy harms.[58]

d) Filter Bubble Transparency Act

On November 9, 2021, a bipartisan group of House lawmakers introduced legislation that would give people more control over the algorithms that shape their online experience.[59] If passed, the Filter Bubble Transparency Act would require companies like Meta to offer a version of their platforms that runs on an "input-transparent" algorithm that doesn't pull on user data to generate recommendations—in other words, provide users with an option to opt out of algorithmic content feeds based on personal data. This House legislation is a companion bill to Senate legislation introduced in June 2021.

e) Deepfake Task Force Act

On July 29, Senators Gary Peters (D-Mich.) and Rob Portman (R-Ohio) introduced bipartisan legislation which would create a task force within the Department of Homeland Security (DHS) tasked with producing a plan to reduce the spread and impact of deepfakes, digitally manipulated images and video nearly indistinguishable from authentic footage.[60] The bill would build on previous legislation, which passed the Senate last year, requiring DHS to conduct an annual study of deepfakes.

6. State and City Regulations

a) 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,[61] state lawmakers and civil rights advocates proposed new rules to prohibit discrimination arising out of automated decision-making by public agencies.[62] 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.[63] If enacted, public agencies in Washington state would be prohibited from using automated decisions 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.

b) New York City Council Bill Passed to Ban Employers from Using Automated Hiring Tools without Yearly Audit to Determine Discriminatory Impact

On November 10, 2021, the New York City Council passed a bill barring AI hiring systems that do not pass annual audits checking for race- or gender-based discrimination.[64] The bill would require the developers of such AI tools to disclose more information about the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

workings of their tool and would provide candidates the option of choosing an alternative process to review their application. The legislation would impose fines on employers or employment agencies of up to $1,500 per violation.

C. Intellectual Property

1. *Thaler v. Hirshfeld*

Intellectual property has historically offered uncertain protection to AI works. Authorship and inventorship requirements are perpetual stumbling blocks for AI-created works and inventions. For example, in the United States, patent law has rejected the notion of a non-human inventor.[65] The Federal Circuit has consistently maintained this approach.[66] This year, the Artificial Inventor Project made several noteworthy challenges to the paradigm. First, the team created DABUS, the "Device for the Autonomous Bootstrapping of Unified Sentience"—an AI system that has created several inventions.[67] The project then partnered with attorneys to lodge test cases in the United States, Australia, the EU, and the UK.[68] These ambitious cases reaped mixed results, likely to further diverge as AI inventorship proliferates.

In the United States, DABUS was listed as the "sole inventor" in two patent applications.[69] In response, the USPTO issued a Notice to File Missing Parts of Non-Provisional Application because the "application data sheet or inventor's oath or declaration d[id] not identify each inventor or his or her legal name" and stressed that the law required that inventorship "must be performed by a natural person."[70] The patent applicants sought review in the Eastern District of Virginia, which agreed with the USPTO.[71] The Artificial Inventor Project faced comparable setbacks in Europe. The European Patent Office ("EPO") rebuffed similar patent applications, holding that the legal framework of the European patent system leads to the conclusion that the law requires human inventorship.[72] The Legal Board of Appeal similarly held that under the European Patent Convention, patents require human inventorship.[73] DABUS fared no better in UK patent courts, which held that the Patents Act requires that an inventor be a person.[74] Conversely, South Africa's patent office granted the first patent for an AI inventor.[75] A leader of the legal team explained the differential outcome: in the UK, the patent application was "deemed withdrawn" for failure to comply associated with filing the patent forms; however, "South Africa does carry out formalities examination, and issued it, as required, on the basis of the designation in the international (Patent Cooperation Treaty [PCT]) application, which was previously accepted by WIPO."[76] Weeks later, the Federal Court of Australia also held that AI inventorship was not an obstacle to patentability.[77] But it is worth noting that Australia's patent system does not employ a substantive patent examination system.

While developments in South Africa and Australia offer encouragement to AI inventors, there is no promise for harmonization. Instead a patchwork approach is more likely. The United States and Europe are likely to maintain the view that AI is an inventor's tool, but not an inventor.

2. *Google LLC v. Oracle America, Inc.*

On April 5, 2021, 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 APIs to build its Android smartphone platform.[78] Notably, the Court did not rule on whether Oracle's APIs 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."[79] 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."[80] The Court focused on Google's

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

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.[81]

While the ruling appears to turn on this particular case, it will likely have repercussions for AI and platform creators.[82] 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.

D. Healthcare

1. FDA's Action Plan for AI Medical Devices

In January 2021, the U.S. Food and Drug Administration (FDA) presented its first five-part Action Plan focused on Artificial Intelligence/Machine Learning (AI/ML)-based Software as a Medical Device (SaMD). The Action Plan is a multi-pronged approach to advance the FDA's oversight of AI/ML-based SaMD, developed in response to stakeholder feedback received from the April 2019 discussion paper, "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device."[83] The FDA's stated vision is that "with appropriately tailored total product lifecycle-based regulatory oversight" AI/ML-based SaMD "will deliver safe and effective software functionality that improves the quality of care that patients receive."[84]

As proposed in the FDA's January 2021 Action Plan, in October 2021 the FDA held a public workshop on how information sharing about a device supports transparency to all users of AI/ML-enabled medical devices.[85] The stated purpose of the workshop was twofold: (1) to "identify unique considerations in achieving transparency for users of AI/ML-enabled medical devices and ways in which transparency might enhance the safety and effectiveness of these devices;" and (2) "gather input from various stakeholders on the types of information that would be helpful for a manufacturer to include in the labeling of and public facing information of AI/ML-enabled medical devices, as well as other potential mechanisms for information sharing."[86]

The workshop had three main modules on (1) the meaning and role of transparency; (2) how to promote transparency; and (3) a session for open public comments.[87] Specific panels covered topics such as patient impressions and physician perspectives on AI transparency, the FDA's role in promoting transparency and transparency promotion from a developer's perspective.[88] After the workshop, the FDA solicited public comments regarding the workshop by November 15, 2021, to be taken into consideration going forward.[89]

2. FDA Launches List of AI and Machine Learning-Enabled Medical Devices

On September 22, 2021, the FDA shared its preliminary list of AI/ML-based SaMDs that are legally marketed in the U.S. via 510(k) clearance, De Novo authorization, or Premarket (PMA) approval.[90] The agency developed this list to increase transparency and access to information on AI/ML-based SaMDs, and to act "as a resource to the public regarding these devices and the FDA's work in the space."[91] The effort comes alongside the growing interest in developing such products to contribute to a wide variety of clinical spheres, and the increasing number of companies seeking to incorporate AI/ML technology into medical devices. The FDA noted that one of "the greatest potential benefits of ML resides in its ability to create new and important insights from the vast

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

amount of data generated during the delivery of health care every day."[92]

E. Autonomous Vehicles ("AVs")

1. U.S. Federal Developments

In June 2021, Representative Bob Latta (R-OH-5) again re-introduced the Safely Ensuring Lives Future Deployment and Research Act ("SELF DRIVE Act") (H.R. 3711), which would create a federal framework to assist agencies and industries to deploy AVs around the country and establish a Highly Automated Vehicle Advisory Council within the National Highway Traffic Safety Administration ("NHTSA"). Representative Latta had previously introduced the bill in September 23, 2020, and in previous sessions.[93]

Also in June 2021, The Department of Transportation ("DOT") released its "Spring Regulatory Agenda," and proposed that NHTSA establish rigorous testing standards for AVs as well as a national incident database to document crashes involving AVs.[94] The DOT indicated that there will be opportunities for public comment on the proposals.

On June 29, 2021, NHTSA issued a Standing General Order requiring manufacturers and operators of vehicles with advanced driver assistance systems (ADAS) or automated driving systems (ADS) to report crashes.[95] ADAS is an increasingly common feature in new vehicles where the vehicle is able to control certain aspects of steering and speed. ADS-equipped vehicles are what are more colloquially called "self-driving vehicles," and are not currently on the market. The Order requires that companies must report crashes within one day of learning of the crash if the crash involved a "a hospital-treated injury, a fatality, a vehicle tow-away, an air bag deployment, or a vulnerable road user such as a pedestrian or bicyclist."[96] An updated report is also due 10 days after the company learned of the crash.[97] The order also requires companies to report all other crashes involving an ADS-equipped vehicle that involve an injury or property damage on a monthly basis.[98] All reports submitted to NHTSA must be updated monthly with new or additional information.[99]

NHTSA also requested public comments in response to its Advance Notice of Proposed Rulemaking ("ANPRM"), "Framework for Automated Driving System Safety," through the first quarter of 2021.[100] The ANPRM acknowledged that NHTSA's previous AV-related regulatory notices "have focused more on the design of the vehicles that may be equipped with an ADS—not necessarily on the performance of the ADS itself."[101] To that end, NHTSA sought input on how to approach a performance evaluation of ADS through a safety framework, and specifically whether any test procedure for any Federal Motor Vehicle Safety Standard ("FMVSS") should be replaced, repealed, or modified, for reasons other than for considerations relevant only to ADS. NHTSA noted that "[a]lthough the establishment of an FMVSS for ADS may be premature, it is appropriate to begin to consider how NHTSA may properly use its regulatory authority to encourage a focus on safety as ADS technology continues to develop," emphasizing that its approach will focus on flexible "performance-oriented approaches and metrics" over rule-specific design characteristics or other technical requirements.[102]

2. Iowa's Automated Vehicle Legislation

In 2019, the Iowa legislature approved a law allowing driverless-capable vehicles to operate on the public highways of Iowa without a driver, if the vehicle meets certain conditions including that the vehicle must be capable of attaining minimal risk if the automated driving system malfunctions. It also requires the vehicle's system to comply with Iowa's traffic laws, and the manufacturer must certify that a manufacturer be in compliance with all applicable federal motor vehicle safety standards.[103] In August 2021, the Iowa Transportation Commission approved rules for automated vehicles. These regulations include requirements that a "manufacturer or entity shall not test driverless-capable vehicles in Iowa without a valid permit," and imposes restrictions on who may

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

qualify for a driverless-capable vehicle permit.[104] It also provides authority to the department to restrict operation of the vehicle "based on a specific functional highway classification, weather conditions, days of the week, times of day, and other elements of operational design while the automated driving system is engaged."[105]

F. Financial Services

Amid the increasing adoption of AI in the financial services space, the year also brought a renewed push to regulate such technological advances. Federal agencies led the charge issuing numerous new regulations and previewing more to come in 2022.

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency teamed up to issue a new cybersecurity reporting rule.[106] The rule applies to all Banking Organizations[107] governed by the agency and compels Banking Organizations to notify their primary Federal regulators within 36 hours of any sufficiently serious "computer-security incident."[108] The rule takes effect in April 1, 2022 and all regulated entities must comply by May 1, 2022.[109]

In addition to newly issued regulations, numerous agencies signaled their desire to regulate technological advances in financial services as soon as early 2022. Five Agencies jointly held an open comment period on "Financial Institutions' Use of Artificial Intelligence" from March 31, 2021, until July 1, 2021, to "understand respondents' views on the use of AI by financial institutions in their provision of services to customers."[110] Kevin Greenfield, Deputy Comptroller for operational risk policy with the OCC, noted that the RFI would specifically shed light on the issue of AI potentially violating consumer protection laws by disparately impacting a protected class, among other issues.[111] This flurry of activity by regulators indicates an active 2022 that might feature several notable new regulations governing the use of advanced technology by various forms of financial services entities.

III. EU POLICY & REGULATORY DEVELOPMENTS

A. European Union

1. EC 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").[112] 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[113] 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

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

risks associated with certain uses of such technology"[114], 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.

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.[115] Therefore, we expect that the proposed rules will not be significantly diluted, and could even be further tightened. 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.

2. EU Parliament AI Draft Report

On November 2, 2021, the EU's Special Committee released its Draft Report on AI in a Digital Age for the European Parliament, which highlights the benefits of use of AI such as fighting climate change and pandemics, and also various ethical and legal challenges.[116] According to the draft report, the EU should not regulate AI as a technology; instead, the type, intensity and timing of regulatory intervention should solely depend on the type of risk associated with a particular use of an AI system. The draft report also highlights the challenge of reaching a consensus within the global community on minimum standards for the responsible use of AI, and concerns about military research and technological developments in weapon systems without human oversight.

3. 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 and published an updated proposal for a new ePrivacy Regulation. 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 contains rules related to the privacy and confidentiality in

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

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.

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.

4. EDPB & EDPS Call for Ban on Use of AI for Facial Recognition in Publicly Accessible Spaces

On June 21, 2021, the European Data Protection Board ("EDPB") and European Data Protection Supervisor ("EDPS") published a joint Opinion calling for a general ban on "any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals, in any context."[117]

In their Opinion, the EDPB and the EDPS welcomed the risk-based approach underpinning the EC's proposed AI Regulation and emphasized that it has important data protection implications. The Opinion also notes the role of the EDPS—designated by the EC's AI Regulation as the competent authority and the market surveillance authority for the supervision of the EU institutions—should be further clarified.[118] Notably, the Opinion also recommended "a ban on AI systems using biometrics to categorize individuals into clusters based on ethnicity, gender, political or sexual orientation, or other grounds on which discrimination is prohibited under Article 21 of the Charter of Fundamental Rights."

Further, the EDPB and the EDPS noted that they "consider that the use of AI to infer emotions of a natural person is highly undesirable and should be prohibited, except for very specified cases, such as some health purposes, where the patient emotion recognition is important, and that the use of AI for any type of social scoring should be prohibited."

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

IV. UK POLICY & REGULATORY DEVELOPMENTS

A. UK Launches National AI Strategy

On September 22, 2021, the UK Government published its 'National AI Strategy' (the "Strategy")[119]. According to the Parliamentary Under Secretary of State at the Department for Digital, Culture, Media and Sport, Chris Philip MP, the aim of the Strategy is to outline "the foundations for the next ten years' growth" to help the UK seize "the potential of artificial intelligence" and to allow it to shape "the way the world governs it"[120]. The Strategy has three pillars: (1) investing in the long-term needs of the AI ecosystems; (2) ensuring AI benefits all sectors and regions; and (3) governing AI effectively.

To that end, the UK aims to attract global talent to develop AI technologies by continuing to support existing academia-related interventions, as well as broadening the routes that talented AI researchers and individuals can work in the UK (for example, by introducing new VISA routes). The UK also seeks to adopt a new approach to research, development and innovation in AI, by, for example, launching a National AI Research and Innovation (R&I) Programme, and also collaborate internationally on shared challenges in research and development (for example, by implementing the US UK Declaration on Cooperation in AI Research and Development.

The Strategy also highlights that effective, pro-innovation governance of AI means that, amongst other things, the UK has a clear, proportionate and effective framework for regulating AI that supports innovation while addressing actual risks and harms. Currently, the UK's regulations for AI are arranged sector by sector ranging from competition to data protection. However, the Strategy acknowledges that this approach can lead to issues including inconsistent approaches across sectors and overlaps between regulatory mandates. To address this, the third pillar outlines key upcoming initiatives to improve AI governance: the Office for AI will publish a White Paper in early 2022, which will outline the Government's position on the potential risks and harms posed by AI systems. The Government will also take other actions including piloting an AI Standards Hub to coordinate UK engagement in establishing AI rules globally, and collaborating with the Alan Turing Institute to provide updated guidance on the ethical and safety issues concerning AI.

B. UK Government Publishes Ethics, Transparency and Accountability Framework for Automated Decision Making

On May 13, 2021, the UK Government published a framework setting out how public sector bodies can deploy automated decision-making technology ethically and sustainably (the "Framework").[121] The Framework segregates automated decision making into two categories: (1) solely automated decision making – decisions that are "fully automated with no human judgment" ; and (2) automated assisted decision making – when "automated or algorithmic systems assist human judgment and decision making." The Framework applies to both types and sets out a seven-step process to follow when using automated decision-making: (1) test to avoid any unintended outcomes or consequences; (2) deliver fair services for all users and citizens; (3) be clear who is responsible; (4) handle data safely and protect citizens' interests; (5) help users and citizens understand

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

how it impacts them; (6) ensure compliance with the law, including data protection laws, the Equality Act 2010 and the Public Sector Equality Duty; and (7) ensure algorithms or systems are continuously monitored and mitigate against unintended consequences.

C. UK Government Publishes Standard for Algorithmic Transparency

Algorithmic transparency refers to openness about how algorithmic tools support decisions. The Cabinet Office's Central Digital and Data Office (the "CDDO") developed an algorithmic transparency standard for Government departments and public sector bodies, which was published on November 29, 2021[122] (the "Standard"). This makes the UK one of the first countries in the world to produce a national standard for algorithmic transparency. The Standard is in a piloting phase, following which the CDDO will review the Standard based on feedback gathered and seek formal endorsement from the Data Standards Authority in 2022.

D. ICO Offers Insight on its Policy Around the Use of Live Facial Recognition in the UK

On June 18, 2021, the Information Commissioner's Office ("ICO") published a Commissioner's Opinion on the use of live facial recognition ("LFR") in the UK ("the Opinion").[123] Facial recognition is the process by which a person can be identified or otherwise recognized from a digital facial image. LFR is a type of facial recognition technology that often involves the automatic collection of biometric data. The Commissioner previously published an opinion in 2019 on the use of LFR in a law enforcement context, concluding that data protection law sets "high standards" for the use of LFR to be lawful when used in public spaces. The Opinion builds on this work by focusing on the use of LFR in public spaces—defined as any physical space outside a domestic setting, whether publicly or privately owned—outside of law enforcement. The Opinion makes clear that first and foremost, controllers seeking to use LFR must comply with the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.

In terms of enforcement, the ICO announced on 29 November 2021 its intention to impose a potential fine of over just £17 million on Clearview AI Inc for allegedly gathering images of a substantial number of people from the UK without their knowledge, in breach of the UK's data protection laws. The ICO also issued a provisional notice to the company to stop further processing the personal data of people in the UK and to delete it. The ICO's preliminary view is that Clearview AI appears to have failed to comply with UK data protection laws in several ways including by failing to have a lawful reason for collecting the information and failing to meet the higher data protection standards required for biometric data under the UK GDPR. Clearview AI Inc will now have the opportunity to make representations in respect of the alleged breaches, following which the ICO is expected to make a final decision. This action taken by the ICO highlights the importance of ensuring that companies are compliant with UK data protection laws prior to processing and deploying biometric data.

E. UK Financial Regulator Vows to Boost Use of AI in Oversight

The UK's Prudential Regulation Authority ("PRA") intends to make greater use of AI, according to its Business Plan for 2021/22.[124] The focus on AI is part of the PRA's aim to follow through on commitments set out in its response to the Future of Finance report (published in 2019) to develop further their RegTech strategy. The Future of Finance report recommended that supervisors take advantage of the ongoing developments in data science and processing power, including AI and machine learning, that automate data collection and processing.[125]

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

F. Consultation on the Future Regulation of Medical Devices in the UK

On September 16, 2021, the Medicines & Healthcare products Regulatory Agency ("MHRA") published a "Consultation on the future regulation of medical devices in the United Kingdom", which ran until November 25, 2021 (the "Consultation").[126] The Consultation invited members of the public to provide their views on possible changes to the regulatory framework for medical devices in the UK, with the aim of developing a future regime for medical devices which enables (i) improved patient and public safety; (ii) greater transparency of regulatory decision making and medical device information; (iii) close alignment with international best practice and (iv) more flexible, responsive and proportionate regulation of medical devices.

The Consultation set out proposed changes for Software as a medical device ("SaMD") including AI as a medical device ("AIaMD"), noting that current medical device regulations contain few provisions specifically aimed at regulating SaMD or AIaMD. The MHRA's proposals therefore include amending UK medical devices regulations in order to both protect patients and support responsible innovation in digital health. Some of the possible changes put forward by the MHRA in the Consultation include (amongst others) defining 'software', clarifying or adding to the requirements for selling SaMD via electronic means, changing the classification of SaMD to ensure the scrutiny applied to these medical devices is more commensurate with their level of risk and more closely harmonised with international practice. The MHRA intends that any amendments to the UK medical device framework will come into force in July 2023.

The MHRA also separately published an extensive work programme on software and AI as a medical device to deliver bold change to provide a regulatory framework that provides a high degree of protection for patients and public, but also to ensure that the UK is the home of responsible innovation for medical device software.[127] Any legislative change proposed by the work programme will build upon wider reforms to medical device regulation brought about by the Consultation.

---

[1] Steven Overly & Melissa Heikkilä, "China wants to dominate AI. The U.S. and Europe need each other to tame it.," Politico (Mar. 2, 2021), available at https://www.politico.com/news/2021/03/02/china-us-europe-ai-regulation-472120.

[2] *Id.*

[3] *Id.*

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

[5] 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/.

[6] *Id.*

[7] 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/.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[8] 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.

[9] 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/.

[10] Dan Reilly, "White House A.I. director says U.S. should model Europe's approach to regulation," Fortune (Nov. 10, 2021), available at https://fortune.com/2021/11/10/white-house-a-i-director-regulation/.

[11] S. 1260, 117th Cong. (2021).

[12] *Id*., §§4201-4207.

[13] *Id*., §4202.

[14] *Id*., §4204. For more details on the NSCAI report and 2020 Executive Order, please see our Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems.

[15] White House, "Join the Effort to Create a Bill of Rights for an Automated Society" (Nov. 10, 2021), available at https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.

[16] Dave Nyczepir, "White House technology policy chief says AI bill of rights needs 'teeth,'" FedScoop (Nov.10, 2021), available at https://www.fedscoop.com/ai-bill-of-rights-teeth/.

[17] *Id.*

[18] Office of Science and Technology Policy, *Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies* (Oct. 8, 2021), *available at* https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.

[19] U.S. Government Accountability Office, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities, Highlights of GAO-21-519SP*, available at https://www.gao.gov/assets/gao-21-519sp-highlights.pdf.

[20] The key monitoring practices identified by the GAO are particularly relevant to organizations and companies seeking to implement governance and compliance programs for AI-based systems and develop metrics for assessing the performance of the system. The GAO report notes that monitoring is a critical tool for several reasons: *first*, it is necessary to continually analyze the performance of an AI model and document findings to determine whether the results are as expected, and *second*, monitoring is key where a system is either being scaled or expanded, or where applicable laws, programmatic objectives, and the operational environment change over time.

[21] Draft NIST Special Publication 1270, *A Proposal for Identifying and Managing Bias in Artificial Intelligence* (June 2021), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270-draft.pdf?_sm_au_=iHVbf0FFbP1SMrKRFcVTvKQkcK8MG.

[22] National Institute of Science and Technology, *Comments Received on A Proposal for Identifying and Managing Bias in Artificial Intelligence (SP 1270)*, available at https://www.nist.gov/artificial-intelligence/comments-received-proposal-identifying-and-managing-

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

bias-artificial.

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

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

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

[26] Defense Innovation Unit, *Responsible AI Guidelines: Operationalizing DoD's Ethical Principles for AI* (Nov. 14, 2021), available at https://www.diu.mil/responsible-ai-guidelines.

[27] 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").

[28] For more information, please see our Artificial Intelligence and Automated Systems Legal Update (1Q21).

[29] S. 1776, 117th Cong. (2021).

[30] S. 1705, 117th Cong. (2021).

[31] *Portman, Heinrich Announce Bipartisan Artificial Intelligence Bills Included in FY 2022 National Defense Authorization Act*, Office of Sen. Rob Portman (Dec. 15, 2021), available at https://www.portman.senate.gov/newsroom/press-releases/portman-heinrich-announce-bipartisan-artificial-intelligence-bills-included.

[32] 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.

[33] 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.

[34] 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.

[35] FTC, *FTC Chair Lina M. Khan Announces New Appointments in Agency Leadership Positions* (Nov. 19, 2021), *available at* https://www.ftc.gov/news-events/press-releases/2021/11/ftc-chair-lina-m-khan-announces-new-appointments-agency.

[36] FTC, *Resolution Directing Use of Compulsory Process Regarding Abuse of Intellectual Property* (Sept. 2, 2021), *available at* https://www.law360.com/articles/1422050/attachments/0. These resolutions were passed by the Democratic commissioners on a 3-2 party line vote. The GOP commissioners issued a dissenting statement, arguing that blanket authorizations remove commission oversight while doing nothing to make investigations more effective.

[37] Ben Brody, *FTC official warns of seizing algorithms 'juiced by ill-gotten data'* (July 27, 2021), *available at* https://www.protocol.com/bulletins/ftc-seize-algorithms-ill-

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

gotten?_sm_au_=iHV5LNM5WjmJt5JpFcVTvKQkcK8MG.

[38] The FTC had previously relied on Section 13(b) to pursue disgorgement via injunctive relief, mostly concerning consumer protection violations. The Supreme Court found, however, that the injunction provision authorized the FTC only to seek a court order halting the illegal activity and did not give it the power to ask a court to impose monetary sanctions. A similar bill, which was introduced the week of the Supreme Court ruling and was endorsed by 25 state attorneys general and President Joe Biden, passed the House over the summer in a nearly party-line vote, but hasn't yet been moved through the Senate. Republicans opposed that initiative over concerns about due process and the bill's 10-year statute of limitations. The new bill, on the other hand, includes a three-year statute of limitations and wording that requires the commission to prove that the company accused of breaking the law did so intentionally.

[39] S. _ 117th Cong. (2022-2023) https://www.law360.com/cybersecurity-privacy/articles/1449355/gop-sen-floats-bill-to-restore-ftc-s-restitution-powers?nl_pk=4e5e4fee-ca5f-4d2e-90db-5680f7e17547&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy

[40] Harry Brignull, the PhD who coined the term "dark patterns" has developed a taxonomy, which may include: trick questions; sneak into basket (in an online purchase, last minute items are added to the basket, without the user's involvement); roach motel (services are easily entered into but difficult to cancel); privacy over-disclosure (users are tricked into sharing or making public more information than intended); price comparison prevention (websites make it difficult to compare prices from other providers); misdirection; hidden costs; bait and switch; confirmshaming (users are guilted into something or a decline option is phrased to shame the users, e.g. "No, I don't want to save money"); disguised ads; forced continuity (free trial unexpectedly turns into a paid subscription); and friend spam (user contact list is used to send unwanted messages from the user). *See* Harry Brignull, *Types of Dark Pattern*, Dark Patterns, *available at* https://www.darkpatterns.org/types-of-dark-pattern.

[41] *Bringing Dark Patterns to Light: An FTC Workshop*, Federal Trade Commission, April 29, 2021, *available at* https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop.

[42] Jon Hill, *CFPB's Newest Hook On Big Tech May Be 1970s Data Law*, Law360 (Nov. 16, 2021), *available at* https://www.law360.com/technology/articles/1439641/cfpb-s-newest-hook-on-big-tech-may-be-1970s-data-law?nl_pk=0d08c9f5-462a-4ad6-9d20-292663da6d5e&utm_source=newsletter&utm_medium=email&utm_campaign=technology.

[43] CFPB, *CFPB Takes Action to Stop False Identification by Background Screeners* (Nov. 4, 2021), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-stop-false-identification-by-background-screeners/?_sm_au_=iHVFR9tfrf49TNNMFcVTvKQkcK8MG.

[44] EEOC, *EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness* (Oct. 28, 2021), *available at* https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness?_sm_au_=iHV5LNM5WjmJt5JpFcVTvKQkcK8MG.

[45] 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.

[46] FTC, Statement of Commissioner Rohit Chopra, *In the Matter of Everalbum and Paravision*, Commission File No. 1923172 (Jan. 8, 2021), *available at*

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf.

[47] *See, e.g., Vance v. Amazon*, 2:20-cv-01084-JLR (W.D. Wash. Oct. 7, 2021); *Vernita Miracle-Pond et al. v. Shutterfly Inc.*, No. 2019-CH-07050, (Ill. Cir. Ct. of Cook County); *Carpenter v. McDonald's Corp.*, No. 2021-CH-02014 (Ill. Cir. Ct. May 28, 2021); *Rivera v. Google, Inc.*, No. 1:16-cv-02714 (N.D. Ill. Aug. 30, 2021); *Pena v. Microsoft Corp.*, No. 2021-CH-02338 (Ill. Cir. Ct. May 12, 2021); *B.H. v. Amazon.com Inc.*, No. 2021-CH-02330 (Ill. Cir. Ct. May 12, 2021), *Pruden v. Lemonade, Inc.*, No. 1:21-cv-07070 (S.D.N.Y. Aug. 20, 2021).

[48] S. _, 117th Cong. (2021); *see also* Press Release, *Senators Markey, Merkley Lead Colleagues on Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology* (June 15, 2021), *available at* https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.

[49] For more details, please see our previous alerts: Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems.

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

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

[52] S. 1896, 117th Cong. (2021); *see also* Press Release, *Senator Markey, Rep. Matsui Introduce Legislation to Combat Harmful Algorithms and Create New Online Transparency Regime* (May 27, 2021), *available at* https://www.markey.senate.gov/news/press-releases/senator-markey-rep-matsui-introduce-legislation-to-combat-harmful-algorithms-and-create-new-online-transparency-regime.

[53] H.R. 3723, 117th Cong. (2021).

[54] Elise Hansen, *House Clears Bill To Study Crypto And Consumer Protection*, Law360 (June 23, 2021), *available at* https://www.law360.com/articles/1396110/house-clears-bill-to-study-crypto-and-consumer-protection.

[55] S. 2134, 117th Cong. (2021); see also Press Release, Office of U.S. Senator Kirsten Gillibrand, Press Release, Gillibrand Introduces New And Improved Consumer Watchdog Agency To Give Americans Control Over Their Data (June 17, 2021), *available at* https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-new-and-improved-consumer-watchdog-agency-to-give-americans-control-over-their-data.

[56] Under the proposed legislation, "personal data" is defined as "electronic data that, alone or in combination with other data—(A) identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, household, or device; or (B) could be used to determine that an individual or household is part of a protected class." Data Protection Act of 2021, S. 2134, 117th Cong. § 2(16) (2021).

[57] *Id*., § 2(3) (2021).

[58] Id., § 2(11)-(13) (2021).

[59] H.R. 5921 (2021), *available at* https://www.congress.gov/bill/117th-congress/house-bill/5921/cosponsors?s=1&r=90&overview=closed; S.B. 2024 (2021), *available*

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

at https://www.congress.gov/bill/117th-congress/senate-bill/2024/text.

[60] U.S. Senate Committee on Homeland Security & Governmental Affairs, *Tech Leaders Support Portman's Bipartisan Deepfake Task Force Act to Create Task Force at DHS to Combat Deepfakes* (July 30, 2021), *available at* https://www.hsgac.senate.gov/media/minority-media/tech-leaders-support-portmans-bipartisan-deepfake-task-force-act-to-create-task-force-at-dhs-to-combat-deepfakes.

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

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

[63] 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/.

[64] N.Y.C., No. 1894-2020A (Nov. 11, 2021), *available at* https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9.

[65] *See Thaler v. Hirshfeld*, No. 120CV903LMBTCB, 2021 WL 3934803, at *8 (E.D. Va. Sept. 2, 2021) (noting "overwhelming evidence that Congress intended to limit the definition of 'inventor' to natural persons.").

[66] See, e.g., *Univ. of Utah v. Max-Planck-Gesellschaft*, 734 F.3d 1315, 1323 (Fed. Cir. 2013); *Beech Aircraft Corp. v. EDO Corp*., 990 F.2d 1237, 1248 (Fed. Cir. 1993).

[67] The Artificial Inventor Project ambitiously describes DABUS as an advanced AI system. DABUS is a "creative neural system" that is "chaotically stimulated to generate potential ideas, as one or more nets render an opinion about candidate concepts" and "may be considered 'sentient' in that any chain-based concept launches a series of memories (*i.e*., affect chains) that sometimes terminate in critical recollections, thereby launching a tide of artificial molecules." Ryan Abbott, *The Artificial Inventor behind this project*, *available at* https://artificialinventor.com/dabus/.

[68] Ryan Abbott, *The Artificial Inventor Project*, *available at* https://artificialinventor.com/frequently-asked-questions/.

[69] *Thaler v. Hirshfeld*, 2021 WL 3934803, at *2.

[70] *Id*. at *2.

[71] *Id*. at *8.

[72] The European Patent Office, *EPO publishes grounds for its decision to refuse two patent applications naming a machine as inventor*, Jan. 28, 2020, *available at* https://www.epo.org/news-events/news/2020/20200128.html.

[73] Dani Kass, *EPO Appeal Board Affirms Only Humans Can Be Inventors*, Law360, Dec. 21, 2021.

[74] Thomas Kirby, UK court dismisses DABUS - an AI machine cannot be an inventor, Lexology, Dec. 14, 2021.

[75] World's first patent awarded for an invention made by an AI could have seismic implications on IP law, University of Surrey, July 28, 2021.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[76] Gene Quinn, *DABUS Gets Its First Patent in South Africa Under Formalities Examination*, IP Watchdog, July 29, 2021, available at https://www.ipwatchdog.com/2021/07/29/dabus-gets-first-patent-south-africa-formalities-examination/id=136116/.

[77] *Thaler v Commissioner of Patents* [2021] FCA 879.

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

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

[80] *Id*. at *20.

[81] See *id*.

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

[83] *See* U.S. Food & Drug Admin., *Artificial Intelligence/Machine Learning (AI-ML)-Based Software as a Medical Device (SaMD) Action Plan* 1-2 (2021), https://www.fda.gov/media/145022/download [hereinafter *FDA AI Action Plan*]; U.S. Food & Drug Admin., *FDA Releases Artificial Intelligence/Machine Learning Action Plan* (Jan. 12, 2021), https://www.fda.gov/news-events/press-announcements/fda-releases-artificial-intelligencemachine-learning-action-plan. *See also* U.S. Food & Drug Admin., *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Discussion Paper and Request for Feedback* (2019), https://www.fda.gov/media/122535/download.

[84] *FDA AI Action Plan*, *supra* note 1, at 1.

[85] U.S. Food & Drug Admin., *Virtual Public Workshop – Transparency of Artificial Intelligence/Machine Learning-enabled Medical Devices* (last updated Nov. 26, 2021) https://www.fda.gov/medical-devices/workshops-conferences-medical-devices/virtual-public-workshop-transparency-artificial-intelligencemachine-learning-enabled-medical-devices.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] U.S. Food & Drug Admin., *Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices* (last updated Sept. 22, 2021), https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices.

[91] *Id.*

[92] *Id.*

[93] As we addressed in previous legal updates, the House previously passed the SELF DRIVE Act (H.R. 3388) by voice vote in September 2017, but its companion bill (the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (“AV START”) Act (S. 1885)) stalled in the Senate. For more details, see our Fourth Quarter and 2020 Annual Review of Artificial Intelligence and Automated Systems.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[94] U.S. Dep't of Transp., Press Release, *U.S. Department of Transportation Releases Spring Regulatory Agenda (*June 11, 2021), available at https://www.transportation.gov/briefing-room/us-department-transportation-releases-spring-regulatory-agenda.

[95] U.S. Dep't of Transp., *NHTSA Orders Crash Reporting for Vehicles Equipped with Advanced Driver Assistance Systems and Automated Driving Systems*, available at https://www.nhtsa.gov/press-releases/nhtsa-orders-crash-reporting-vehicles-equipped-advanced-driver-assistance-systems

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] 49 CFR 571, available at https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/ads_safety_principles_anprm_website_version.pdf

[101] *Id.*, at 6.

[102] *Id.*, at 7-8.

[103] SF 302, Reg. Session (2019-2020).

[104] ARC 5621C, Notice of Intended Action, available at https://rules.iowa.gov/Notice/Details/5621C.

[105] *Id.*

[106] Carly Page, *US Banks Must Soon Report Significant Cybersecurity Incidents Within 36 Hours*, (Nov. 19, 2021), available at https://techcrunch.com/2021/11/19/us-banks-report-cybersecurity-incidents/?guccounter=1.

[107] "Banking Organizations" is a defined term in the rule and applies to a slightly different mix of entities with respect to each agency.

[108] 86 Fed. Reg. 66424.

[109] *Id*. at 66438.

[110] 86 Fed. Reg. 16837.

[111] Al Barbarino, *Bank Regulators Eye Updated Guidance to Fight Bias in AI* (Oct. 21, 2021), available at https://www.law360.com/cybersecurity-privacy/articles/1433299/.

[112] 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.

[113] 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.

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

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[115] 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".

[116] Draft Report on AI in a Digital Age for the European Parliament (Nov. 2, 2021), available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/AIDA/PR/2021/11-09/1224166EN.pdf

[117] *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence*, available at https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

[118] EDPS, Press Release, *EDPB & EDPS Call For Ban on Use of AI For Automated Recognition of Human Features in Publicly Accessible Spaces, and Some Other Uses of AI That Can Lead to Unfair Discrimination* (June 21, 2021), available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en?_sm_au_=iHVWn7njFDrbjJK3FcVTvKQkcK8MG.

[119] UK Government, *National AI Strategy* (22 September 2021), available at https://www.gov.uk/government/publications/national-ai-strategy.

[120] UK Government, *New ten-year plan to make the UK a global AI superpower* (22 September 2021), available at https://www.gov.uk/government/news/new-ten-year-plan-to-make-britain-a-global-ai-superpower.

[121] UK Government, *Ethics, Transparency and Accountability Framework for Automated Decision-Making* (13 May 2021), available at https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making.

[122] UK Government, *UK government publishes pioneering standard for algorithmic transparency* (November 29, 2021), available at https://www.gov.uk/government/news/uk-government-publishes-pioneering-standard-for-algorithmic-transparency--2.

[123] UK Government, Information Commissioner's Office, *The use of live facial recognition technology in public places* (June 18, 2021), available at https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.

[124] UK Gov't, *Prudential Regulation Authority Business Plan 2021/22* (May 24, 2021), available at https://www.bankofengland.co.uk/prudential-regulation/publication/2021/may/pra-business-plan-2021-22.

[125] UK Gov't, *Future of Finance*, Bank of England (June 2019), available at https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report.pdf?la=en&hash=59CEFAEF01C71AA551E7182262E933A699E952FC.

[126] UK Gov't, *Consultation on the future regulation of medical devices in the United Kingdom* (Sept. 16, 2021), available at https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom.

[127] UK Gov't, *Software and AI as a Medical Device Change Programme* (Sept. 16, 2021), available at

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme.

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Frances Waldmann, Emily Lamm, Tony Bedel, Kevin Kim, Brendan Krimsky, Prachi Mistry, Samantha Abrams-Widdicombe, Leon Freyermuth, Iman Charania, and Kanchana Harendran.

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)

© 2022 Gibson, Dunn & Crutcher LLP Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.

Related Capabilities

Artificial Intelligence

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**