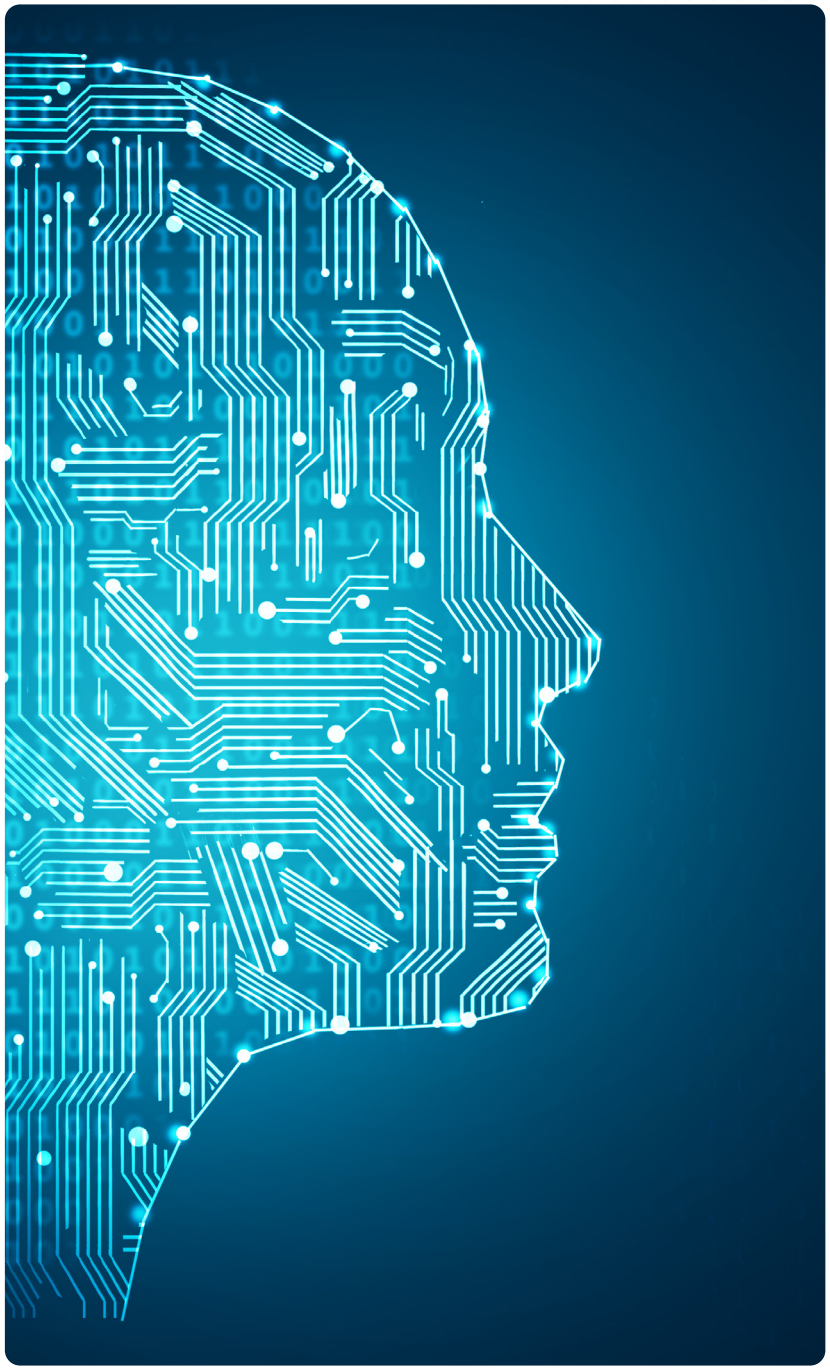


Photo by Peshkova on Shutterstock

LEXOLOGY
Getting the Deal Through

Market Intelligence

ARTIFICIAL INTELLIGENCE 2022

Global interview panel led by Lisa Peets, Sam Jungyun Choi and Jiayen Ong of Covington & Burling LLP

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by Covington & Burling LLP, this Artificial Intelligence volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Government strategies
Ethics & human rights
Data protection & privacy
Industry sector application

START READING

About the editors



Lisa Peets, Sam Jungyun Choi and Jiayen Ong
Covington & Burling LLP

Lisa Peets leads the technology regulatory practice in Covington & Burling's London office and is a member of the firm's Management Committee. Ms Peets divides her time between London and Brussels, and her practice embraces regulatory counsel and legislative advocacy. In this context, she has worked closely with leading multinationals in a number of sectors, including some of the world's best-known technology companies.

Sam Jungyun Choi is an associate in the technology regulatory group in the Brussels office. Her practice focuses on European data protection law and new policies and legislation relating to innovative technologies such as artificial intelligence, online platforms, digital health products and autonomous vehicles. Ms Choi advises leading technology and life sciences companies on a wide range of matters relating to data protection and cybersecurity issues.

Jiayen Ong is an associate in the technology regulatory group in the London office. She has experience across a broad range of technology regulatory issues, with a focus on European data protection law and recent policies and legislation regarding innovative technologies.

Contents

While reading, click this icon to return to the Contents at any time

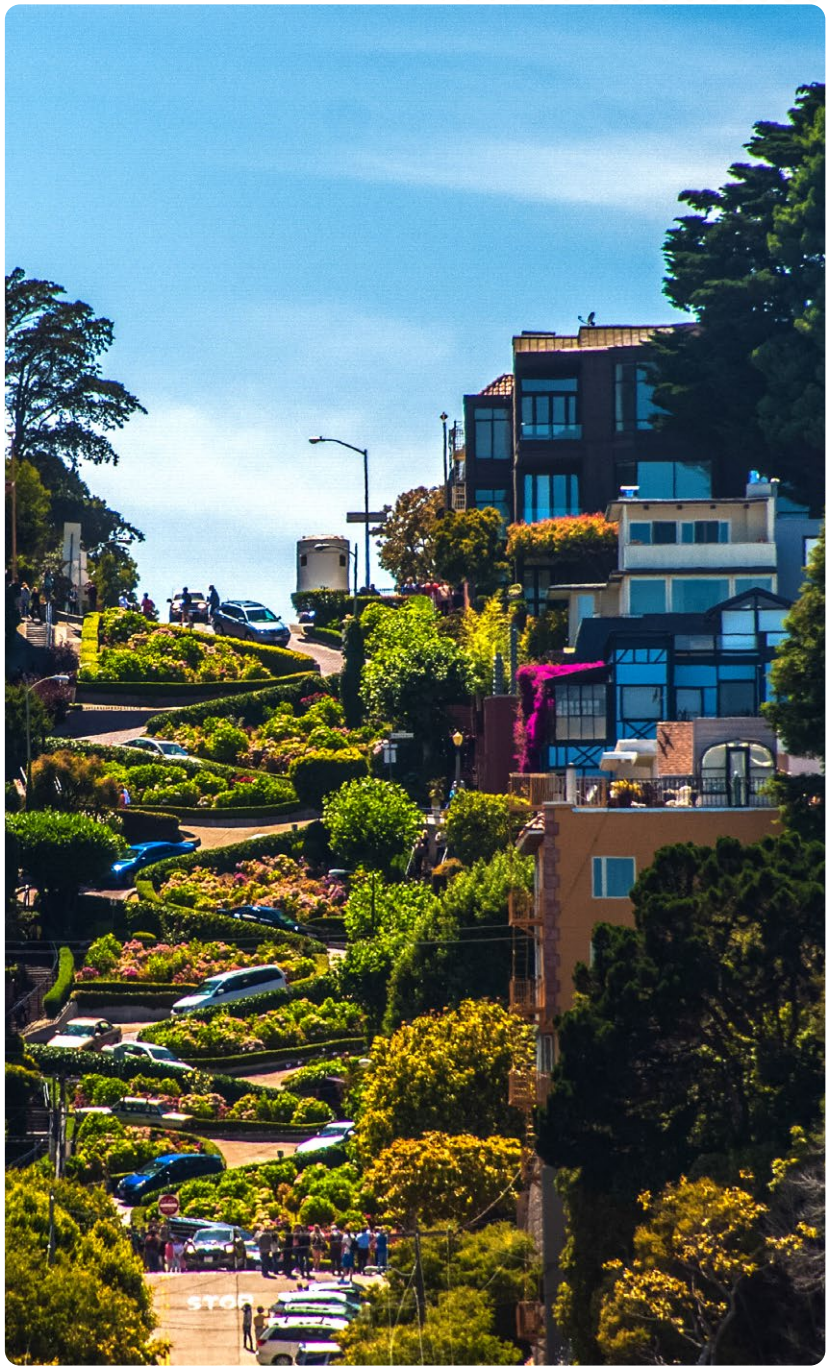


Photo by Maks Ershov on Shutterstock

United States

Lindsey Tonsager is co-chair of Covington's global data privacy and cybersecurity practice. She advises clients in their strategic and proactive engagement with the Federal Trade Commission, the US Congress, the California Privacy Protection Agency and state attorneys general on proposed changes to data protection laws, and regularly represents clients in responding to investigations and enforcement actions involving their privacy and information security practices. Lindsey's practice focuses on helping clients launch new products and services that implicate the laws governing the use of artificial intelligence, data processing for connected devices, biometrics and new technologies, among many others.

Jayne Ponder is an associate in Covington's Washington office. She counsels national and multinational companies across industries on data privacy, cybersecurity and emerging technologies. In particular, Jayne advises clients on compliance with federal, state and global privacy frameworks, and counsels clients on navigating the rapidly evolving legal landscape. Her practice includes partnering with clients on the design of new products and services, and helping clients design governance programmes for the development and deployment of artificial intelligence and internet of things technologies.

Olivia Vega is an associate in Covington's Washington office. She is a member of the data privacy and cybersecurity and healthcare practice groups. Olivia Vega provides strategic advice to global companies on a broad range of privacy, healthcare and technology issues, including in technology transactions, mergers and acquisitions, and regulatory compliance. Olivia counsels clients on navigating federal and state privacy and data security laws and regulations, including on topics such as HIPAA and the California Consumer Privacy Act.

1 What is the current state of the law and regulation governing AI in your jurisdiction? How would you compare the level of regulation with that in other jurisdictions?

Currently, the United States does not have any comprehensive federal laws or regulations that specifically regulate AI. However, as in other jurisdictions, a range of existing US laws, regulations and agency guidance may apply (or may come into effect to apply) to AI, including the following:

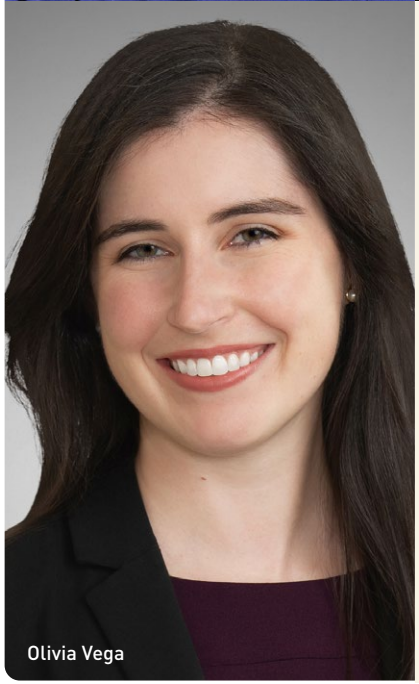
- the United States Federal Trade Commission (FTC) has issued guidance with respect to AI and algorithms, and this guidance highlights existing US laws, regulations and guidance that apply to these technologies;
- the Department of Defense (DOD) has reaffirmed its Ethical Principles for Artificial Intelligence;
- the Food and Drug Administration (FDA) has initiatives aimed at addressing specific AI applications;
- the Department of Energy (DOE) established an AI Advancement Council to lead AI innovation and ethics at the department;
- the Department of Commerce and the Committee on Foreign Investment in the United States (CFIUS) have various requirements applicable to AI; and
- various states and local governments have begun turning their attention to AI regulation.

At the state level, a few states have enacted legislation that will govern automated decision-making, as described further in response to question 5.

While there have been various AI legislative proposals introduced in Congress, the United States has not embraced a horizontal broad-based approach to AI regulation as proposed by the European Commission. Rather, the United States has focused on legislation


Lindsey Tonsager


Jayne Ponder


Olivia Vega

"The United States has continued to focus on funding and developing dedicated projects for AI research."

"The NDAA for Fiscal Year 2021 includes a number of other provisions expanding research, development and deployment of AI such as authorising $1.2 billion through FY 2025 for a DOE artificial intelligence research programme."

investing in infrastructure to promote the growth of AI. In particular, the National Defense Authorization Act (NDAA) for fiscal year 2021 established the National AI Initiative to coordinate the ongoing AI research, development, and demonstration activities among stakeholders. To implement the AI Initiative, the NDAA mandates the creation of a National Artificial Intelligence Initiative Office under the White House Office of Science and Technology Policy (OSTP) to undertake the AI Initiative activities, as well as an interagency National Artificial Intelligence Advisory Committee (NAIAC) to coordinate federal activities pertaining to the AI Initiative.

Since the passage of the AI Initiative, the United States has continued to focus on funding and developing dedicated projects for AI research. For example, the Consolidated Appropriations Act of 2022 requires the Director of National Intelligence to develop a plan, within one year, for an 'artificial intelligence digital ecosystem' that improves the intelligence community's use of 'artificial intelligence-powered applications' and includes appropriations for the armed forces to recruit and train an 'artificial intelligence-literate acquisition workforce'. Additionally, the DOE recently announced the establishment of the Artificial Intelligence Advancement Council, which will lead artificial intelligence governance, innovation and AI ethics at the department, and the DOE pledged to issue US$10 million to support certain research making use of AI techniques. Furthermore, the NDAA for Fiscal Year 2022 authorises the Secretary of Defense to carry out a pilot programem to establish data repositories for DOD data sets relevant to the development of AI technology, and allows certain private and public sector organisations to access those data sets for the purpose of developing AI technology for DOD.

2 Has the government released a national strategy on AI? Are there any national efforts to create data sharing arrangements?

On 11 February 2019, President Trump signed an executive order (EO) 'Maintaining American Leadership in Artificial Intelligence', which launched a coordinated federal government strategy for AI. The EO sets forth the following five pillars for AI:

- empowering federal agencies to drive breakthroughs in AI research and development;
- establishing technological standards to support reliable AI systems;
- establishing governance frameworks to foster public confidence in AI;
- training an AI-ready workforce; and
- engaging with international partners.

Pursuant to the EO, the Trump administration released the Draft AI Regulatory Guidance, and the National Institute for Standards and Technology (NIST) released a plan for developing AI standards.

In addition to this EO, Congress has passed legislation that will have significant implications on AI. Specifically, in addition to the establishing the National AI Initiative, discussed above, the NDAA for Fiscal Year 2021 directs NIST to support the development of relevant standards and best practices pertaining to both AI and data sharing. To support these efforts, Congress has appropriated US$400 million to NIST through FY 2025. The NDAA for Fiscal Year 2021 also has several AI-related provisions pertaining to the DOD. For example, in relation to the Joint Artificial Intelligence Center, the new law requires an assessment and report on whether AI technology acquired by the DOD is developed in an ethically and responsibly sourced manner, including steps taken or resources required to mitigate any deficiencies. Finally, the NDAA for Fiscal Year 2021 includes a number of other provisions expanding research, development and deployment of AI such as authorising $1.2 billion through FY 2025 for a DOE artificial intelligence research programme.

The NDAA for Fiscal Year 2022 further authorises the Secretary of Defense to 'take such actions as may be necessary to increase the number of commercial artificial intelligence companies eligible to provide support to DOD components, including with respect to requirements for cybersecurity protections and processes'. It also requires the Secretary of Defense to review potential AI applications to DOD platforms, processes and operations, and to establish performance objectives and metrics for incorporating AI into such platforms, processes and operations.

The White House has also expressed a commitment to AI development and launched AI.gov and the National AI Research Resource Task Force to coordinate and accelerate AI research across all scientific disciplines. The Task Force released its interim report on 25 May 2022, which lays out its vision — a shared research infrastructure that would provide experts with tools and resources to foster AI research and development. The Department of Commerce also formally launched NAIAC, discussed above, which is tasked with advising the President on a range of issues related to AI, including United States AI competitiveness, issues related to the AI workforce, and AI research and development. The Department of Commerce announced the 27 members of the NAIAC, which include representatives from civil society, academia and industry.

Photo by Francesco Carucci on Shutterstock

3 What is the government policy and strategy for managing the ethical and human rights issues raised by the deployment of AI?

The United States adopted the Organisation for Economic Co-operation and Development (OECD) AI Principles in May 2019, which also were embraced by the G20, focusing on:

- using AI to stimulate inclusive growth, sustainable development and well-being;
- human-centred values and fairness;
- AI transparency and explainability;
- making AI secure, robust and safe throughout its life cycle; and

"Foreign investors must carefully evaluate any investments involving US businesses to determine whether a CFIUS filing may be mandatory or, if not mandatory, warranted on the basis of potential national security risk."

- accountability.

In October 2022, the OSTP published a new blueprint for an 'AI Bill of Rights'. The blueprint is 'intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems'.

The blueprint outlines a set of five principles: (1) safe and effective systems; (2) algorithmic discrimination protections; (3) data privacy; (4) notice and explanation; and (5) alternative options. The blueprint is non-binding and does not constitute US government policy. Nevertheless, the blueprint outlines the White House's vision for the deployment of automated systems.

The Department of Justice (DOJ) and Equal Employment Opportunity Commission (EEOC) each released guidance documents explaining how algorithms and AI can lead to disability discrimination in hiring that violates the Americans with Disabilities Act on 12 May 2022. The guidance documents also provide information to help organisations avoid such discrimination.

The DOD has formally adopted and reaffirmed its own ethical AI principles leveraging the Defense Innovation Board's 2019 report proposing high-level recommendations for ethical use of AI by the DOD. Additionally, the National Security Commission on AI released its own highly anticipated final report in 2019 that, consistent with the DOD's principles, centred on the importance of reliability, auditability, and fairness of AI systems used in the defence context.

4 What is the government policy and strategy for managing the national security and trade implications of AI? Are there any trade restrictions that may apply to AI-based products?

Trade controls are an important and evolving component of AI regulation in the United States and increasingly are being used to manage the cross-border flow of AI technologies. To pursue national security and foreign policy objectives, the United States employs a number of regulatory systems to govern international trade in hardware, software and technology. These regulations are becoming increasingly complex and difficult to navigate, as the United States and China heighten their competition in the technology sector.

The Department of Commerce's Bureau of Industry and Security (BIS) regulates the export, re-export and transfer (in-country) of certain commercial, dual-use and less sensitive military items. In late 2018, BIS published a representative list of 14 categories of 'emerging technologies,' including AI and machine learning, over which it may, in the future, seek to exercise export controls. The very first such 'emerging technology' control was promulgated in January 2020, imposing export restrictions on certain software specially designed for training 'deep convolutional neural networks' to automate the analysis of geospatial imagery. More 'emerging technology' controls

are expected on a rolling basis, and may include additional AI-related export controls.

The Department of Commerce also is authorised to prohibit the export of items subject to the Export Administration Regulations (EAR) to designated foreign parties that pose risks to US interests. Among the parties added to the 'Entity List' pursuant to this authority are several of China's leading AI companies, including Hikvision, iFLYTEK, Megvii Technology, SenseTime and Yitu Technologies, which were designated in 2019 in connection with alleged ties to human rights abuses. A licence issued by BIS is required to export even non-sensitive hardware, software or technology subject to the EAR to these companies.

Separately, inbound investment into AI technologies is under increased scrutiny from national security-focused regulators. CFIUS, an interagency committee composed of nine federal agencies and offices with US national security responsibilities, and chaired by the Department of the Treasury, reviews foreign investments in US businesses that could implicate US national security. Recent legislation and regulations expanding the scope of CFIUS's authorities to address new and evolving threats to US national security, including perceived threats from China, among other things, have focused on US technology development and competition. The changes to the CFIUS regime also included the introduction of a mandatory filing process for certain investments and control transactions involving 'TID US Businesses'.

A company may be a TID US Business if it produces, designs, tests, manufactures, fabricates or develops one or more 'critical technologies,' or maintains or collects 'sensitive personal data'. Businesses involved in AI could fall into one or both of these categories. 'Critical technologies' are defined by reference to certain US export control regulations, including the EAR and there are potential components or applications of AI that could trigger this

Photo by f11photo on Shutterstock

definition. Moreover, AI development relies on significant amounts of data, including data that may be considered 'sensitive personal data.' Foreign investors must carefully evaluate any investments involving US businesses to determine whether a CFIUS filing may be mandatory or, if not mandatory, warranted on the basis of potential national security risk.

5 How are AI-related data protection and privacy issues being addressed? Have these issues affected data sharing arrangements in any way?

There is no comprehensive federal privacy legislation in the United States, and US federal policy has not focused specifically on the data protection and privacy impacts of AI technologies to date. However, there is federal sector-specific privacy legislation regulating, for instance, health data and financial data. Additionally, the FTC has broad jurisdiction to enforce deceptive and unfair business practices,

including privacy and data security practices. In connection with its enforcement efforts, the FTC has recently expressed an interest in requiring companies to delete algorithms and derived learnings when they were created using personal information that was unlawfully collected or used.

In the absence of comprehensive federal privacy legislation, various states have enacted privacy legislation, most notably the California Privacy Rights Act (CPRA), which amends the California Consumer Privacy Act and which broadly regulates privacy and data security practices for companies processing California residents' information. Virginia, Colorado, Utah, and Connecticut have enacted similar privacy legislation. There likely will continue to be more state privacy laws so long as there is no federal privacy legislation pre-empting such state laws. The lack of federal legislation and the need to comply with a patchwork of state and local rules can make compliance more challenging.

The Virginia, Colorado, and Connecticut privacy laws allow consumers to opt out of the processing of personal data for the purposes of 'profiling' in furtherance of decisions that produce legal or similarly significant effects concerning the consumers, and the laws further define profiling as any form of automated processing of personal information. Notably, the Connecticut law limits the opt-out to profiling 'in furtherance of solely automated decisions'. In California, the CPRA authorises the California Privacy Protection Agency to enact regulations governing 'opt-out rights with respect to businesses' use of automated decision making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision making processes, as well as a description of the likely outcome of the process with respect to the consumer'. Regulations related to these issues are expected to be finalised by the end of the year.

"The FTC AI Guidance cautions that the manner in which data is collected for AI use could potentially give rise to liability. For example, the FTC investigated and settled with Everalbum, Inc in January 2021 in relation to its 'Ever App', a photo and video storage app that used facial recognition technology to automatically sort and 'tag' users' photographs."

In addition to broad privacy legislation, states also are considering technology- or sector-specific regulations. Colorado enacted a law that prohibits an insurer from directly or indirectly using an algorithm or predictive model that unfairly discriminates against an individual based on membership in a protected class. Illinois amended its Artificial Intelligence Video Interview Act to provide that employers relying solely upon AI to determine whether an applicant will qualify for an in-person interview must gather and report certain demographic information to the state authorities. The state authorities must then analyse the data and report on whether the data discloses a racial bias in the use of AI. In addition to these examples of enacted legislation, several states have proposed legislation detailed in response to question 10.

6 How are government authorities enforcing and monitoring compliance with AI legislation, regulations and practice guidance? Which entities are issuing and enforcing regulations, strategies and frameworks with respect to AI?

While there has not been comprehensive US AI legislation, agencies are focusing on how existing laws, regulations and guidance might apply to AI, including in the enforcement context. For example, at the federal level, the FTC released a guidance document on 19 April 2021 (the FTC AI Guidance) that discusses existing FTC guidance that already applies to AI and algorithms and outlines five principles for AI and algorithm use. The FTC AI Guidance mentions that certain AI applications must comply with the Fair Credit Reporting Act, the Equal Credit Reporting Act and Title VII of the Civil Rights Act of 1964. More recently, the FTC issued an Advanced Notice of Proposed Rulemaking (ANPRM) on 11 August 2022, the first step in creating trade regulation rules under its section 18 authority, that solicits input on several questions related to automated decision-making technologies. A violation of a trade rule results in civil penalties, so if the FTC were to create new rules for automated decision-making technologies, this could provide a significant source of new requirements.

Photo by Orhan Cam on Shutterstock

The FTC AI Guidance cautions that the manner in which data is collected for AI use could potentially give rise to liability. For example, the FTC investigated and settled with Everalbum, Inc in January 2021 in relation to its 'Ever App', a photo and video storage app that used facial recognition technology to automatically sort and tag users' photographs. Pursuant to the settlement agreement, Everalbum was required to 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. Enforcement activity by the FTC may become even more common, as legislative efforts seek to create a new privacy-focused bureau within the FTC and expand the agency's civil penalty authority. The FTC also has demonstrated its role in this area by hosting hearings and workshops, such as its workshop in April 2021 on how AI may be used to personalise and serve 'dark patterns' to individuals consumers.

> "In the financial sector, large banks report success in implementing AI to improve processes for anti-money laundering and know-your-customer regulatory checks."

Other agencies are considering sector-specific regulation. For example, various federal financial agencies solicited a request for information on financial institutions' use of AI, including machine learning, with the expectation of future regulations. The FDA released its 'Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan', which includes developing a tailored regulatory framework for AI- and machine learning-based SaMD, advising on best practice for the development of machine learning algorithms, and supporting patient transparency.

7 Has your jurisdiction participated in any international frameworks for AI?

As noted above, the United States joined the 'Principles of Artificial Intelligence' adopted by the OECD and the G20. On 15 June 2020, the United States announced its participation in the Global Partnership on AI (GPAI), an effort launched during 2020's G7 ministerial meeting on science and technology, which aims to enhance multi-stakeholder cooperation in the advancement of AI reflecting shared democratic values, with an initial focus on responding to covid-19. The GPAI will initially be comprised of four working groups focused on responsible AI, data governance, the future of work, innovation and commercialisation.

8 What have been the most noteworthy AI-related developments over the past year in your jurisdiction?

The most noteworthy AI developments at the federal level include the FTC's ANPRM on commercial surveillance and the proposed federal privacy legislation. As discussed above in response to question 6, the FTC's ANPRM seeks comment on algorithmic decision-making systems, including on issues such as algorithmic errors, consumer benefits and potential harms. The ANPRM follows on the heels of the FTC's 16 June 2022 report, where the FTC advised that although AI can serve as a helpful tool, there are significant risks associated with its use, particularly as applied to historically disadvantaged communities.

The American Data Privacy and Protection Act (ADPPA), introduced on 21 June 2022, would require 'large data holders' that use algorithms to conduct 'algorithm impact assessments' on certain algorithms that could negatively impact individuals. These assessments must provide details about the design of the algorithm and the data used by the algorithm, as well as a description of steps the large data holder is taking to mitigate harms to individuals. Separately, developers of algorithms are required to conduct 'algorithm design evaluations' that evaluate the design, structure, and inputs of the algorithm.

In addition to these federal developments, a number of state laws will regulate automated decision-making in certain applications. As described in response to question 5, a number of state laws will

afford consumers the ability to opt out of certain automated decision-making starting in 2023. In addition to these more general consumer privacy laws, some states have passed sector-specific laws. For example, Colorado law prohibits an insurer from directly or indirectly using any external consumer data and information source, algorithm, or predictive model that unfairly discriminates against an individual based on membership in a protected class. In addition to these targeted laws, some states, including Alabama, Colorado, Illinois and Vermont have passed bills creating a commission, task force or oversight position to evaluate the use of AI in their states and make recommendations regarding its use.

9 Which industry sectors have seen the most development in AI-based products and services in your jurisdiction?

As a result of the covid-19 pandemic, efforts within the healthcare industry to develop AI-based products and services have accelerated. In addition to the covid-19 response, many other US industries are actively engaging in AI development, including for healthcare financial services, logistics and transportation. In healthcare, for example, digital therapeutics, such as clinical-grade sensors paired with AI-driven predictive analytics are a major area of growth. In the financial sector, large banks report success in implementing AI to improve processes for anti-money laundering and know-your-customer regulatory checks. Additionally, paired with developments in mobile devices and biometrics, financial institutions reportedly are investing in more robust multifactor authentication measures using technologies such as facial recognition. AI also has tremendous potential to assist with supply chain and inventory management and other logistics.

Photo by f11photo on Shutterstock

10 Are there any pending or proposed legislative or regulatory initiatives in relation to AI?

While various federal legislative proposals have been introduced, such as the ADPPA discussed above, it is unlikely that any will pass in the near term given other priorities of the administration. In addition to the ADPPA, Congress is also considering the United States Innovation and Competition Act of 2021, which would incorporate AI-related provisions of several other bills introduced over the past year, including the AI Jobs Act of 2022, AI in Counterterrorism Oversight Enhancement Act and Fellowships and Traineeships for Early-Career AI Researchers Act.

Notably, there has been increased interest in ensuring the safe use of algorithms with children, as evidenced by recent legislative efforts. For example, at the federal level, the Kids Online Safety Act would impose new safeguards, tools and transparency requirements for minors online, and would create a duty for covered entities to

> "Companies should closely monitor state and federal legal developments and consider engaging with policymakers on AI legislation and regulatory developments to inform legal efforts in this area."

act in the best interests of minors using their products, and would apply to commercial software that connects to the internet and is likely to be used by a minor. Affected companies, to the extent they operate 'algorithmic recommendation systems' that use minors' personal data, would be required to make disclosures in its terms and conditions that disclose how those algorithmic recommendation systems are used by the covered platform to provide information to minors and information about options for minors and their parents to control algorithmic recommendation systems that use minor's data. Similarly, the recently enacted California Age-Appropriate Design Code will prohibit affected businesses from using personal information to 'profile a child' by default unless the business can demonstrate appropriate safeguards to protect children, and either (1) the profiling is necessary to provide the product of feature with which the child is actively and knowingly engaged, and (2) the business can demonstrate a compelling reason that profiling is in the best interest of children. 'Profiling' is defined as 'any form of automated processing' of personal information, including analysing or predicting aspects of a person.

In addition, a continuing area of emerging consensus is support of AI-related research and training. The AI Training Act would the Director of the Office of Management and Budget to develop an AI training programme for certain federal workers, including those involved in procurement, logistics, programem management, research and development, and cost estimating. The training should include information related to the science underlying AI, as well as the risks posed by AI, 'including discrimination and risks to privacy'.

There continues to be a growing body of state and federal proposals that address algorithmic accountability and mitigation of unwanted bias and discrimination. Federal proposals include the Health Equity and Accountability Act of 2022, which aims to address algorithmic bias in the context of healthcare and would require the Secretary of the Department of Health and Human Services to establish a Task Force on Preventing AI and Algorithmic Bias in Healthcare to develop guidance on how to ensure that the development and use of AI and algorithmic technologies in delivering care 'does not exacerbate health disparities' and help ensure broader access to care. Other federal bills, such as the Digital Platform Commission Act of 2022, would establish the Federal Digital Platform Commission, which is empowered to develop regulations for online services that facilitate interactions between consumers, and between consumers and entities offering goods and services. Such regulations could include, for example, requirements that algorithms used by the platforms 'are fair, transparent, and without harmful, abusive, anticompetitive, or deceptive bias'.

Relatedly, NIST released for public comment a draft of its AI Risk Management Framework, which provides guidance for managing risks in the design, development, use and evaluation of AI systems. In particular, the Framework addresses 'characteristics of

trustworthiness' such as accuracy, explainability, reliability, security and privacy. NIST separately released a document titled 'Towards a Standard for Identifying and Managing Bias within Artificial Intelligence', which aims to provide guidance for mitigating harmful bias within AI systems.

States are considering their own slate of related proposals. For example, states continue to propose bills to create oversight bodies that would review and report on states' use of AI and other automated decision-making systems and develop recommendations for the use of these systems. Additionally, facial recognition technology continues to attract attention from state lawmakers, with wholesale bans on state and local government agencies' use of facial recognition gaining steam.

11 What best practices would you recommend to assess and manage risks arising in the deployment of AI?

Companies developing or deploying AI applications in the United States should be mindful that a number of existing laws, regulations and regulatory guidance may apply to their AI application – including, but not limited to, those discussed above. Companies should seek to ensure compliance with these existing requirements and guidance, and review decisions of any governmental authorities that may be relevant to their offering. Companies should also closely monitor state and federal legal developments and consider engaging with policymakers on AI legislation and regulatory developments to inform legal efforts in this area. To the extent that companies are offering services outside the United States, they should expand these practices to other jurisdictions.

Although the legal landscape with respect to AI is still evolving, companies can take steps now to help manage potential risks that may arise when developing or deploying AI, as we discuss our article '10 Steps To Creating Trustworthy AI Applications' (www.covingtondigitalhealth.com/2020/05/7415/). These steps involve, among other things, adopting a governance framework to help build on and operationalise the applicable AI principles and help ensure compliance with laws and applicable practices.

Lindsey Tonsager
ltonsager@cov.com

Jayne Ponder
jponder@cov.com

Olivia Vega
ovega@cov.com

Covington & Burling LLP
San Francisco, Washington DC
www.cov.com

Read more from this firm on Lexology

The Inside Track

What skills and experiences have helped you to navigate AI issues as a lawyer?

At Covington, we take a holistic approach to AI that integrates our deep understanding of technology matters and our global and multi-disciplinary expertise. We have been working with clients on emerging technology matters for decades, and we have helped clients navigate evolving legal landscapes, including at the dawn of cellular technology and the internet. We draw upon these past experiences as well as our deep understanding of technology and leverage our international and multi-disciplinary approach. We also translate this expertise into practical guidance that clients can apply in their transactions, public policy matters and business operations.

Which areas of AI development are you most excited about and which do you think will offer the greatest opportunities?

The development of AI technology is affecting virtually every industry and has tremendous potential to promote the public good, including to help achieve the UN Sustainable Development Goals by 2030. For example, in the healthcare sector, AI may continue to have an important role in helping to mitigate the effects of covid-19, and it has the potential to improve outcomes while reducing costs, including by aiding in diagnosis and policing drug theft and abuse. AI also has the potential to enable more efficient use of energy and other resources and to improve education, transportation, and the health and safety of workers. We are excited about the many great opportunities presented by AI.

What do you see as the greatest challenges facing both developers and society as a whole in relation to the deployment of AI?

AI has tremendous promise to advance economic and public good in many ways and it will be important to have policy frameworks that allow society to capitalise on these benefits and safeguard against potential harm. Also, as this publication explains, several jurisdictions are advancing different legal approaches with respect to AI. One of the great challenges is to develop harmonised policy approaches that achieve desired objectives. We have worked with stakeholders in the past to address these challenges with other technologies, such as the internet, and we are optimistic that workable approaches can be crafted for AI.