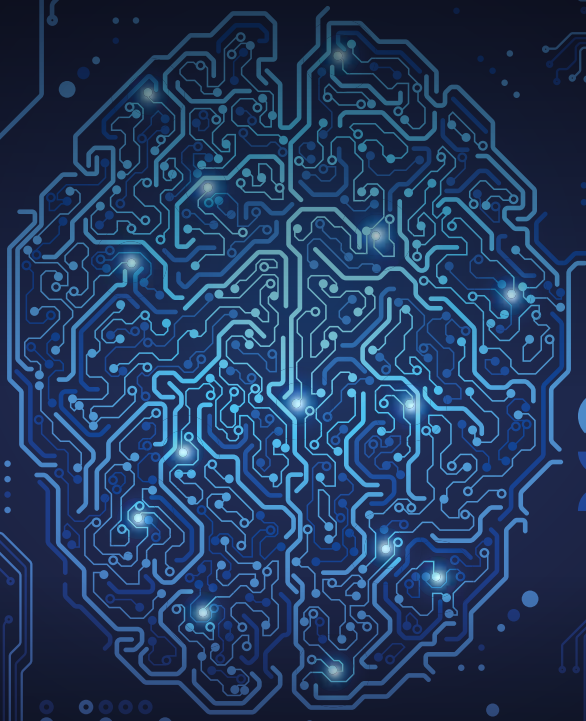
Market Intelligence

ARTIFICIAL INTELLIGENCE 2021

Global interview panel led by Covington & Burling LLP



LEXOLOGY
Getting the Deal Through

LEXOLOGY
Getting the Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/g/
Jakarin+Niamklang

ISBN: 978-1-83862-734-8

Printed and distributed by Encompass Print Solutions

ARTIFICIAL INTELLIGENCE 2021

United States

Lee Tiedrich is co-chair of Covington's global and multi-disciplinary artificial intelligence initiative and brings together an undergraduate education in electrical engineering and over 25 years of experience to counsel clients on a broad range of intellectual property, technology transactions, AI governance, data, policy and other matters. She has written and spoken extensively on AI, including at the Council on Foreign Relations, at the Singapore Embassy (with the ambassador) and with the Federal Judicial Conference, the Aspen Institute and the Society of Corporate Secretaries and Governance Professionals.

Terrell McSweeny is a partner with Covington's multi-disciplinary artificial intelligence initiative. A former Commissioner of the Federal Trade Commission (FTC), she has held senior appointments in the White House, Department of Justice (DOJ), and the US Senate. Her practice focuses on antitrust and consumer protection including counseling clients in a variety of areas of technology law. Ms McSweeny is internationally recognised for her work at the intersection of law and policy with cutting-edge technologies.

James Yoon is an associate in Covington's Washington office. He is a member of the data privacy and cybersecurity and commercial litigation practice groups. Mr Yoon advises clients on a broad range of privacy, cybersecurity, and consumer protection issues, including compliance obligations, incident preparedness and response, and defending against regulatory inquiries. As part of Covington's AI Initiative, he advises clients on the evolving regulatory landscape for AI and implementation of trustworthy AI principles into their organisations and product life cycles.

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 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.

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. The United States has instead focused on legislation investing in infrastructure to promote the growth of AI. In particular, the National Defense Authorization Act (NDAA), which became effective January 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 to coordinate federal activities pertaining to the AI Initiative. The White House also launched AI.gov and the National AI Research Resource Task Force to coordinate and accelerate AI research across all scientific disciplines.


Lee Tiedrich


Terrell McSweeny


James Yoon

"The United States has not embraced a horizontal broad-based approach to AI regulation."

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 NIST released a plan for developing AI standards.

On 1 January 2021, Congress enacted the NDAA, which represents the most substantial federal US legislation on AI to date and will have significant implications. In addition to the establishing the National AI Initiative, discussed in question 1, the NDAA 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 $400 million to NIST through FY 2025. The NDAA 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 includes a number of other provisions expanding research, development and deployment of AI such as authorising $1.2 billion through FY 2025 for a Department of Energy artificial intelligence research programme.

Finally, the National Security Commission on AI (NSCAI) released its final report proposing a national strategy for AI, with particular focus on the importance of domestic investment in innovation and education. The report explains what the United States must do to defend against the spectrum of AI-related threats, and recommends how the US government can responsibly use AI technologies in defense. The report further addresses AI competition and recommends actions the government must take to promote AI innovation to improve international competitiveness.

"Recently, the White House OSTP announced its plan to develop a 'bill of rights' to protect American consumers of harmful applications and consequences of AI."

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
- accountability.

Recently, the White House OSTP announced its plan to develop a 'bill of rights' to protect American consumers of harmful applications and consequences of AI. The OSTP hinted that enumerating rights is the first step and more prescriptive regulations may be forthcoming — such as the federal government refusing to buy software or technology that fail to follow the 'bill of rights.' In support of this plan,

Photo by Sean Pavone on Shutterstock

the OSTP has issued a request for information specifically seeking information about biometrics and other AI-based technologies used to identify people and infer attributes.

The DOD has formally adopted and recently 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, as discussed in question 2, the NSCAI released its own highly anticipated final report this year 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 regulates the export, re-export or transfer (in-country) of certain US defence and dual-use items. In late 2018, the Bureau 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 ban the supply of US-origin items–or of foreign-made items that contain or that were produced based on US-origin content or technology–to designated foreign end-users, if those end-users 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. These companies now require a specific licence from the Department of Commerce to receive even non-sensitive hardware, software or technology subject to US export controls jurisdiction.

Separately, inbound investment into AI technologies is under increased scrutiny from national security-focused regulators. The Committee on Foreign Investment in the United States (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, has manifested in the space of technology development and competition. In turn, the changes to the CFIUS regime included the introduction of a mandatory filing process for certain investments into a 'TID US Business.' A TID US Business includes a company that produces, designs, tests, manufactures, fabricates, or develops 'critical technologies' as well as companies that collect, process or store 'sensitive personal data'. Businesses involved in AI could fall into one or both of these categories. On the technology side, there are potential components or applications of AI that could

> "In addition to broad privacy legislation, states also are considering technology or sector specific regulations."

trigger the 'critical technology' definition, and the regulations cross-reference both export control classifications and the emerging technologies list issued by BIS. At the same time, AI development relies on significant amounts of data, including data that may be considered 'sensitive personal data.'

The national security concerns around AI do not stop with CFIUS, however. The NSCAI released its report earlier this year strongly signaling that the US is behind and needs to invest significant resources on technology development and the advancement of AI. The White House has also issued two separate Executive Orders focused on securing the Information and Communications Technology and Services (ICTS EO) and connected software applications (Applications EO). Commerce has issued an Interim Final Rule implementing the ICTS EO, which allows Commerce to prohibit or restrict certain transactions between US companies and foreign providers that involve ICTS and that are not otherwise subject to CFIUS jurisdiction and review. The Commerce Department has yet to issue a proposed rulemaking for the Applications EO, but similar to the ICTS EO, the Applications EO seeks to mitigate the potential risk of a foreign party of concern accessing significant US

data through a connected software application and in turn, may seek to restrict US transactions with foreign parties in that space as well.

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 the absence of comprehensive federal privacy legislation, various states have enacted privacy legislation, most notably the California Privacy Rights Act, which replaces the California Consumer Privacy Act and which broadly regulates privacy and data security practices for companies processing California residents' information. Virginia and Colorado 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.

In addition to broad privacy legislation, states also are considering technology or sector specific regulations. Colorado recently 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, on the federal level, the FTC released a guidance document on 19 April 2021 (the FTC AI Guidance), which 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.

The FTC AI Guidance also 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

Photo by B R O N on Shutterstock

its workshop in April 2021 on how AI may be used to personalise and serve 'dark patterns' to individuals consumers.

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 is exploring a new Proposed Regulatory Framework for AI- and machine learning-based software as a medical device that includes issuance of guidance on a predetermined change control plan for software's learning over time, best practice for the development of machine learning algorithms, device transparency and real-world monitoring pilot programs.

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, and 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 NDAA and related actions arising from the National AI Initiative, the FTC's AI Guidance and related actions, and trade controls regulations.

It also is noteworthy that the US Patent and Trademark Office (USPTO), the US Copyright Office and the World Intellectual Property Organization are looking at issues pertaining to the protection of AI-related or generated intellectual property. Indeed, the USPTO released the Artificial Intelligence Patent Dataset in July 2021, identifying which of the 13.2 million United States patents and pre-grant publications include AI.

In addition to these federal developments, states and localities have also taken important steps, including with respect to privacy and facial recognition technology, as discussed, and other actions discussed in question 10.

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.

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

While various federal legislative proposals have been introduced, it is unlikely that any will pass in the near term given other priorities of the administration.

Notably, one area of emerging consensus is support of AI-related research and training. The AI Training Act (S 2551) would require the Office of Management and Budget to establish an AI training programme for employees of executive agencies responsible for acquisition. The Artificial Intelligence for the Military Act of 2021 (S 1776) would require the introduction of curriculum for professional military education to incorporate courses of emerging technologies, such as AI.

A growing body of state and federal proposals address algorithmic accountability and mitigation of unwanted bias and discrimination. Federal proposals directed at algorithmic accountability include the SAFE DATA Act, which would require the FTC to conduct a study examining the use of algorithms to process data and requires the FTC to refer cases to appropriate agencies where algorithms were used to violate civil rights laws. The Mind Your Own Business Act of 2021 (S 1444) would authorise the FTC to promulgate regulations that would require covered entities to, among other requirements, conduct impact assessments of 'high-risk automated decision systems,' such as artificial intelligence and machine learning techniques, and 'high-risk information systems' that 'pose a significant risk to the privacy or security' of consumers' personal information. Other federal bills, like the Algorithmic Justice and Online Platform Transparency Act of 2021 (S 1896), would subject online

> "One area of emerging consensus is support of AI-related research and training."

platforms to transparency requirements such as describing to users the types of algorithmic processes they employ and the information they collect to power them and publishing annual public reports detailing their content moderation practices.

States are considering their own slate of related proposals. For example, the California State Assembly is considering the Automated Decision Systems Accountability Act of 2021, which would require monitoring and impact assessments for California businesses that provide 'automated decision systems', defined broadly as products or services using artificial intelligence or other computational techniques to make decisions. A Washington state bill (SB 5116) would direct the state's chief privacy officer to adopt rules regarding the development, procurement and use of automated decision systems by public agencies. More broadly, facial recognition technology has attracted renewed 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.

Lee Tiedrich
ltiedrich@cov.com

Terrell McSweeny
tmcsweeny@cov.com

James Yoon
jyoon@cov.com

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

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.

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.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Government strategies
Ethics and human rights
Data protection & privacy
Risk & compliance management

ISBN 978-1-83862-734-8