wiley

NEWSLETTER

Top 4 Areas to Watch in 2021 in AI Legal and Regulatory Risks

December 2020

Privacy in Focus®

Artificial intelligence (AI) technology and applications have been expanding over the last few years, and in 2021, we expect government agencies to ramp up their efforts to deal with the actual and perceived impacts of the technology. Government scrutiny will expand across a range of sectors, and industry stakeholders will need to engage to ensure that the benefits of the technology are highlighted, while also focusing on approaches to mitigate implementation risks. Indeed, the current Administration has laid the groundwork for further AI scrutiny, and the next Administration appears likely to delve deeper.

Below, we highlight four key areas where we expect significant AI activity in the coming year that will have wide-ranging impacts on private-sector entities that develop and deploy AI.

1. *Requirements That Every Federal Agency Develop an AI Regulatory Plan by May 2021*

The current Administration released AI regulatory guidance in November 2020 – in the form of a memorandum from the Office of Management and Budget (OMB) – that calls for a relatively light-touch approach to AI regulation at the federal level. It instructs agencies to prioritize consideration of non-regulatory approaches and encourages the use of voluntary frameworks, such as the National Institute of Standards and Technology (NIST) cybersecurity and privacy frameworks. The memorandum stems from a February 2019 Executive Order on AI that launched the American AI Initiative (American AI Initiative EO), and defined the Administration's overall

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Artificial Intelligence (AI)

Privacy, Cyber & Data Governance

approach to AI.

The guidance embodies a risk-based approach to AI regulation, suggesting that greater regulation may be appropriate in certain high-risk areas. Specifically, the guidance suggests approval of "narrowly tailored and evidence-based regulations [to] address specific and identifiable risks" in some circumstances, for purposes of enhancing public trust and ensuring U.S. competitiveness. Accordingly, the guidance leaves the door open for AI regulation to address issues like privacy or safety, as well as regulation in specific use cases (e.g., facial recognition technology or autonomous vehicles) or to address specific issues (e.g., algorithmic content moderation and "deep fakes") – though any regulation should still be tied to an assessment of the risk of actual harm and the costs that come with any regulation.

Notably, the OMB memorandum also creates a new requirement for federal agencies, including independent agencies such as the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), to develop agency plans to implement its guidance. These plans, which must be publicly posted, are due to the Office of Information and Regulatory Affairs (OIRA) on May 17, 2021, meaning that agencies will be working to develop plans on approaches to AI regulation as they transition leadership. This requirement on federal agencies represents an important opportunity for stakeholders to engage with new and existing agency leadership as each agency develops a comprehensive plan for AI regulation that will likely telegraph agency priorities.

2. *NIST Trustworthy AI Standards*

NIST has been very active on AI issues, particularly since the Administration's February 2019 Executive Order. In August 2019, NIST released its Plan for federal engagement and U.S. leadership on AI standards, and it describes that it will participate in developing AI standards, including by "[s]upporting and conducting AI research and development[;] [a]ctively engaging in AI standards development[;] [p]rocuring and deploying standards-based products and services[;] and [d]eveloping and implementing supportive policies, including regulatory policies where needed."

Looking forward, NIST's work to develop these standards and tools for "trustworthy" AI will begin to yield additional work product in 2021. Specifically, in 2021, NIST will (or likely will):

- Finalize guidance on the key issue of **explainability** – the concept that AI algorithms should produce explanations for their outcomes or conclusions, at least under some circumstances. NIST has already released and sought comment on a draft version of NISTIR 8312, which outline four principles that "comprise the fundamental properties for explainable AI systems." In January, NIST is scheduled to host a virtual workshop to "delve further into developing an understanding of explainable AI," which will inform the final version of NISTIR 8312.
- Seek public engagement on AI **bias** – in furtherance of ongoing research to understand, measure, and ultimately mitigate bias in AI systems. NIST has already hosted one workshop on this issue, and we expect NIST will put out a report on AI bias in 2021, "detailing a taxonomy of concepts and defining terminology in the field of AI bias," drawing in part from the earlier workshop.

- Continue work on research around AI **security**. Already, NIST's National Cybersecurity Center of Excellence (NCCoE) has published draft work on adversarial machine learning – the act of malicious actors misleading or giving malicious inputs to machine learning systems. Given that the public comment period on this draft closed nearly a year ago – in January 2020 – it is likely that this work will be finalized soon. Additionally, NIST has stated that its "plans include investing an additional $1.4 million in FY2021 to develop a reference architecture, example solutions, and best practices for securing AI." Ultimately, this may tie into the concept of "resiliency" in AI, and lead to the development of new tools and standards for securing AI systems.

All of these efforts present opportunities for private-sector engagement with NIST, a non-regulatory federal agency with a long-standing history of engaging with industry and other stakeholders. Ultimately, NIST has expressed plans to develop a more comprehensive, risk-based framework – like it has done with the Cybersecurity Framework and the Privacy Framework – for AI standards. That risk-based framework would incorporate the work on explainability, bias, and security, noted above, and would have a broad reach and major impacts on the AI ecosystem. As such, it is critical that industry continue to collaborate with NIST to ensure flexible, voluntary, and risk-based approaches.

3. *Federal Agency Trustworthy Principles*

On December 3, 2020, the outgoing President signed a new Executive Order on AI – Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (Trustworthy AI Principles EO) – which, among other things, sets out principles for most federal agencies to use in implementing AI technology themselves. These principles are consistent with AI principles that the Administration has promoted in both its domestic and international efforts on AI governance, and are designed to promote public trust in AI. While these do not directly impact private-sector AI systems – as they apply to agencies' own uses of AI – we expect that the principles will have a ripple effect throughout the broader AI ecosystem and will influence agencies' approaches to AI more generally, as they are more developed than OMB's guidance from even a month before.

Specifically, the Trustworthy AI Principles EO holds that "[w]hen designing, developing, acquiring, and using AI in the Federal Government, agencies shall adhere to the following Principles":

- Lawful and respectful of our Nation's values.
- Purposeful and performance-driven.
- Accurate, reliable, and effective. Agencies shall ensure that their application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.
- Safe, secure, and resilient.
- Responsible and traceable.
- Regularly monitored.

Further, the Trustworthy AI Principles EO imposes additional requirements on covered agencies with respect to AI – including a requirement to develop and implement plans for all agency AI systems to either be consistent with the principles or retired. As with the regulatory plans that agencies will need to develop, the development of these plans to ensure agency AI is consistent with the principles will spill over into the new Administration and represent opportunities for industry to engage with agency leadership on key issues.

4. *FTC Enforcement Activity Focusing on AI*

Finally, 2021 will almost certainly see increased scrutiny on AI and data-driven algorithms from the FTC. Already, the FTC under the current Administration has made clear its role – through enforcement – in ensuring the "transparent, explainable, fair, and empirically sound" use of AI tools.

This activity is likely to see a significant increase under the Biden Administration's FTC. Both of the Democratic Commissioners – Commissioner Chopra and Commissioner Slaughter – have expressed specific interest in and have been critical of AI and data-driven algorithms. For example, Commissioner Slaughter, in a January 2020 speech, laid out her proposed approach to AI, and noted:

Terms such as machine-learning, math, code, and data hold out the tantalizing prospect of objective, unbiased, and superior decision-making. Some of this promise bears out. But we also know that algorithmic decisions still produce biased and discriminatory outcomes. We have seen mounting evidence of AI-generated economic harms in employment, credit, healthcare, and housing.

Pointing to concerns such as faulty inputs, faulty conclusions, failure to test, and proxy discrimination, Commissioner Slaughter laid out a path toward what she terms "algorithmic justice" to remedy "serious harm to consumers and undermine rather than advance economic justice." In part, she has called for greater AI transparency, which "must, at a minimum, be coupled with increased accountability and appropriate remedies," explaining that "[i]ncreased accountability means that companies ... must bear the responsibility of (1) conducting regular audits and impact assessments, and (2) facilitating appropriate redress for erroneous or unfair algorithmic decisions."

Likewise, Commissioner Chopra has focused on the potential for algorithms to produce discriminatory outcomes, as well as the lack of algorithmic transparency, particularly in advertising and marketing decisions. If either Commissioner becomes Chair, they will have the ability to set the investigative and policy priorities for the agency very quickly, and their clear concern over the potential harms from AI could become FTC priorities, even more than they are today.

***

To be sure, there are other areas that are ripe for action in 2021 with respect to AI, spanning potential national security restrictions, existing and proposed regulations of facial recognition technology at different levels of government, proposed approaches to algorithmic content moderation, and international engagement with Europe and others on cross-national AI regulation – which we have covered elsewhere and will continue to cover in future articles. In sum, 2021 promises to be an active year as the legal and regulatory

risks associated with developing and deploying AI for private-sector actors take shape.

Our Artificial Intelligence Practice counsels clients on AI compliance, risk management, and regulatory and policy approaches, and we engage with key government stakeholders in this quickly moving area. Please reach out to a member of our team with any questions.