wiley

NEWSLETTER

Key Commission on AI Recommends Privacy and Civil Liberties Protections in Domestic AI Uses

March 2021

Privacy In Focus®

On March 1, 2021, the National Security Commission on Artificial Intelligence (NSCAI) released its final report and submitted it to Congress. The NSCAI was established by Congress to make recommendations on how to approach AI from a national security standpoint – and the Commission did not leave many stones unturned. As anticipated, the report recommends "an integrated national strategy," outlined in a two-pronged approach addressing national security measures and international technology competition on AI. Its recommendations are divided into 16 sections and include draft legislative text and Executive Orders.

Of particular note, the final report recommends that the government take certain domestic actions to protect privacy, civil rights, and civil liberties in its AI deployment. The Commission expressed concern that lack of public trust in AI from a privacy or civil rights/civil liberties standpoint will undermine the ability to develop and deploy AI to promote U.S. intelligence, homeland security, and law enforcement. The report therefore advocates for government agencies to lead the way in their approach to AI on these issues – which may directly affect how AI is deployed in the private sector as well.

Report Recommendations

The NSCAI final report outlines a broad array of recommendations. Part I, "Defending America in the AI Era" (Chapters 1-8), outlines what the United States must do to defend against the spectrum of AI-

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Artificial Intelligence (AI)
Privacy, Cyber & Data Governance

related threats from state and non-state actors and recommends how the U.S. government can responsibly use AI technologies to protect the American people and the nation's interests. Part II, "Winning the Technology Competition" (Chapters 9-16), outlines AI's role in broader technology competition.

A number of key domestic policy considerations are contained in a chapter on "Upholding Democratic Values: Privacy, Civil Liberties, and Civil Rights in Uses of AI for National Security." The report notes that "[p]ublic trust will hinge on justified assurance that government use of AI will respect privacy, civil liberties, and civil rights." In particular, the report recommends the creation of a task force to address these issues and outlines efforts through which the government can establish and ensure that its use of AI tools is effective, including:

- Developing AI tools to enhance oversight and auditing;
- Increasing public transparency about AI use;
- Building AI systems that advance the goals of privacy preservation and fairness;
- Ensuring that those impacted by government actions involving AI can seek redress and have due process.

A key set of recommendations focuses on increasing public transparency about the government's AI use through improved reporting. For example, it recommends that Congress require AI Risk Assessment Reports and AI Impact Assessments to assess the privacy, civil liberties, and civil rights implications for each new qualifying AI system or significant system refresh that involves U.S. persons. And it further recommends that the President act in this area if Congress does not do so.

Another set of recommendations would encourage agencies to develop and test AI systems with goals of privacy preservation and fairness. This would include the requirement of having national security agencies implement steps to mitigate privacy, civil liberties, and civil rights risks associated with any AI system on an iterative basis and require documentation of all accepted risks. Each covered agency would also need to designate an office, committee, or team in each agency to conduct a pre-deployment review of AI technologies that will impact privacy, civil liberties, and civil rights.

A third set of recommendations would go further and implement government mechanisms to provide for individuals to seek redress and due process for alleged violations of their rights due to AI operation. It recommends that the FBI and the U.S. Department of Homeland Security (DHS) conduct reviews to ensure that individuals can seek redress based on use of AI, and that the U.S. Department of Justice independently issue guidance on AI and due process.

Finally, the final report recommends strengthening oversight and governance mechanisms. This includes strengthening the U.S. Privacy and Civil Liberties Oversight Board's (PCLOB) ability to provide meaningful oversight and advice on the federal government's use of AI-enabled technologies for counterterrorism purposes, and providing a greater role for the DHS offices of Privacy and Civil Rights and Civil Liberties. The report also suggest that the President or Congress establish a task force to assess the privacy and civil rights and civil liberties implications of AI and emerging technologies.

Future Implications

The Commission has been widely praised on a bipartisan basis in Congress, and it remains to be seen which of its many recommendations gain traction in the new Administration and Congress. But its emphasis on domestic privacy, civil rights, and civil liberties protections – as a component of national security – is likely to resonate beyond just national security policy.

Policymakers and stakeholders have been looking at tools to examine privacy and fairness in AI, and they may start by ordering agency reviews of their own AI deployment. Even now, the National Institute of Standards and Technology (NIST) is working on standards to facilitate this review. Much of the government remains concerned that "trust" in AI is necessary for widespread AI deployment, and these expectations may well impact the private sector as well.