Volume 4, No. 4 | July–August 2021

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 4, No. 4 | July–August 2021

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

National Security Commission on Artificial Intelligence Final Report Prioritizes U.S. Global Competition, Conflict Preparation, and Enhanced Protection of Privacy and Civil Liberties

Katherine Sheriff and K.C. Halm*

After two years of research, analysis, briefings, stakeholder engagements, and committee deliberations the National Security Commission on Artificial Intelligence has issued its Final Report on a national strategy to leverage artificial intelligence. The authors of this article explain the report and next steps.

Authorized by the 2019 Defense Authorization Act, the National Security Commission on Artificial Intelligence ("NSCAI" or "Commission") has been working for two years to develop a comprehensive national strategy to leverage artificial intelligence ("AI") to enhance national security, expand AI adoption and development, and continue to prevail in the international AI technology competition "arms race." Now after two years of research, analysis, briefings, stakeholder engagements, and committee deliberations the NSCAI has issued its final report to Congress and the president (the "Final Report").[1]

The Final Report opens with a stark message: the government is not organized or resourced to win the technology competition against a committed competitor, nor is it prepared to defend against AI-enabled threats, or to rapidly adopt AI applications for national security purposes. The language of the Final Report makes clear the Commission's intention to deliver this message with real urgency. The NSCAI asserts the nation must be "AI Ready" in less than four years, by 2025, to defend and compete in the coming era of AI-accelerated competition and conflict. As the Commission explains:

Robotics, Artificial Intelligence & Law / July–August 2021, Vol. 4, No. 4, pp. 243–250.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

> The United States should invest what it takes to maintain its innovation leadership, to responsibly use AI to defend free people and free societies, and to advance the frontiers of science for the benefit of all humanity. AI is going to reorganize the world.
>
> America must lead the charge.

Overview

The Final Report outlines an integrated national strategy to meet the goals of "AI Readiness" by 2025 and maintain AI leadership. Divided into two parts, "Defending America in the AI Era" and "Winning the Technology Competition," the Final Report outlines urgent actions needed to reorganize the government, reorient the nation, and rally our closest allies and partners to defend and compete in the coming AI era.

Part 1 addresses emerging national security threats in AI, with a focus on AI in warfare and the use of autonomous weapons, AI in intelligence gathering, and "upholding democratic values in AI." This latter principle, which focuses on privacy, civil liberties, and civil rights in use of AI for national security, may have significant implications for potential oversight and regulation of private sector AI. Part 2 provides a strategy for winning the technology competition, with a focus on securing talent, promoting innovation, protecting IP rights, and related concepts.

The Final Report's recommendations surrounding the concept of "upholding democratic values" identify specific domestic policy action to protect privacy, civil liberties, and civil rights when the government is deploying AI systems. These actions include using tools such as AI risk and impact assessments, audits and tests of AI systems, and mechanisms for providing due process and redress to individuals adversely affected by AI systems used in government. If implemented these recommendations could be extended to the private sector, which would have a significant impact on the development and use of this emerging technology.

NSCAI Recommendations to Defend America and Win the Technology Competition

Organized in two parts, the Final Report presents a series of recommendations under two frameworks: actions needed to defend America in the AI era, and actions necessary to ensure that the United States wins the global competition and AI arms race.

Part 1: "Defending America in the AI Era"

The Commission identifies a number of action items necessary to defend against emerging AI-enabled threats to America's free and open society. Key themes include:

Prepare for Future Warfare and Manage Risks of AI-Enabled and Autonomous Weapons

At the top of the list is a recommendation that the Department of Defense ("DoD") achieve a state of AI military readiness by 2025, and manage risks associated with AI-enabled and autonomous weapons by affirming U.S. policy that only human beings can authorize employment of nuclear weapons (and seeking commitments from Russia and China to follow that policy) and developing international standards of practice for the development, testing, and use of AI-enabled and autonomous weapon systems. DoD must also establish foundations for widespread integration of AI by 2025 by building a common digital infrastructure, developing a digitally literate workforce, and instituting more agile acquisition budgeting and oversight processes.

Transform National Intelligence and Expand Talent

The Commission recommends that the intelligence community adopt and integrate AI-enabled capabilities across all aspects of its work, from collection to analysis. In addition, intelligence and national security agencies need new talent, which could be addressed by implementing digital service academies, and digital "corps" (similar to the Army Medical Corps) to organize AI technologists serving in government.

Present a "Democratic Model" of AI Use for National Security

The Final Report affirms that AI tools are critical for U.S. intelligence, homeland security, and law enforcement agencies. However, the public's trust in the use of AI to support the missions of these agencies rests on assurance that government use of AI will respect privacy, civil liberties, and civil rights. In a recent Congressional hearing focused on NSCAI recommendations, Commission Chairman Schmidt testified that, "In the face of digital authoritarianism," the United States must present a "democratic model of responsible use of AI for national security. The trust of our citizens will hinge on justified assurance that the government's use of AI will respect privacy, civil liberties and civil rights." Recommendations in support of this goal include the following:

- *Improve Public Transparency Regarding Government's Use of AI*. To do so the Commission recommends that Congress should "require AI Risk Assessment Reports and AI Impact Assessments" from key federal agencies, including the Federal Bureau of Investigation, Department of Homeland Security, and the intelligence community. Additionally, the Final Report recommends that the National Institute of Standards and Technology provide and regularly refresh a set of standards, performance metrics, and tools for "qualified confidence" in AI models, data, and training environments and predictive outcomes.
- ***Develop and Test Systems with the Goal of Advancing Privacy Preservation and Fairness***. These recommendations include requiring national security agencies to take proactive steps to assess and mitigate potential risks by testing AI systems, assessing AI/machine learning model performance on an ongoing basis, and using privacy-preserving technology (such as anonymization). The Commission also recommends that the government "establish third-party testing centers for national security-related AI systems that could impact U.S. persons."
- *Strengthen Individuals' Rights to Redress and Due Process When Impacted by Government Action Involving AI*. To achieve this outcome the Final Report concludes that it is important for agencies to ensure opportunities for redress, consistent with the constitutional principle of due process,

> are available to persons affected by government action involving AI, which should include an analysis of whether adequate notice of AI use in decision making is provided to impacted parties, as well as the "degree to which AI systems can be audited" to trace the process by which a system arrived at a recommendation (if contested). Further, this recommendation also calls for the attorney general to issue guidance on AI and due process to describe how relevant agencies should safeguard the due process rights of U.S. persons when AI use may lead to a deprivation of life or liberty.

The Commission's decision to issue recommendations beyond national security, and focus on domestic policy issues around privacy and civil liberties may impact future policy making over private-sector oversight and governance. A number of policy makers are weighing the utility of tools such as audits, impact assessments, and reporting requirements for AI-enabled decision-making systems. The endorsement of such tools in the Final Report may lead other policy makers to adopt such regulatory tools for private-sector use and development of AI systems. Further, the emphasis on ensuring sufficient redress and due process rights could carry over to the continuing debate and policy proposals addressing transparency, explainability, and the so-called "black box" problem of AI.

On the back end, the Final Report recommends establishing policies that allow individuals to raise concerns about irresponsible AI development and adopt oversight and enforcement practices, which should include "auditing and reporting requirements," a review system for "high-risk" AI systems, and an appeals process for those affected.

Part 2: "Winning the Technology Competition"

Competition with China to research, develop, and deploy AI is intensifying. While the United States retains advantages in critical areas, the Final Report concludes that "current trends are concerning."

The Commission identifies a number of action items necessary to defend against emerging AI-enabled threats to America's and the world's free and open societies. Key themes include:

Leadership

The Commission finds that the U.S. government is not prepared because it lacks the structured leadership to accelerate the U.S. government's integration of AI. To remedy this problem the Final Report proposes a White House Technology Competitiveness Council reporting into the vice president to "precisely monitor and drive this transformation."

Talent Deficit

The huge talent deficit in the U.S. government requires decisive action. Specifically, the U.S. government needs to:

- Build new digital talent pipelines;
- Expand existing programs;
- Cultivate AI nationwide; and
- Ensure the most talented technologists come to the United States and stay in the United States and do not go to our competitors.

Encompassing these priorities, the proposed Digital Services Academy would establish an accredited, degree-granting university in which students would receive a highly technical education tuition-free. Graduates would enter the government as civil servants with a five-year service obligation, helping meet the government's needs for expertise in AI, software engineering, electrical engineering, computational biology, and several other areas.

Semiconductor Reliance

Hardware development in the United States is heavily reliant on semiconductor manufacturing in East Asia and Taiwan. Most cutting-edge plants come from a specific plant 110 miles from China; Chairman Schmidt noted in recent Congressional testimony that this "must be an issue." The United States must revitalize cutting-edge manufacturing and implement a national microelectronics strategy. The Final Report states unequivocally that the objective is to stay two generations ahead of Chinese efforts.

Innovation Investment

Because AI research is very expensive, the Final Report recommends that the U.S. government set conditions for broad-based

innovation across the country. Chairman Schmidt explained recently: "We need a National AI Research Infrastructure so more than the top five companies have the resources to innovate," particularly universities and start-ups. The Final Report also recommends spending up to $40 billion in annual funding within the next five years to cover AI research and development for defense and non-defense purposes.

Next Steps: Feedback, Hearings, and Further Questions About AI Integration and Use

The NSCAI welcomes further review and feedback on the Final Report's recommendations. Citing the partnership with the broader AI and AI-adjacent community as a critical factor in their work, the NSCAI hopes to continue this cooperation as it moves forward into the next and arguably most important phase of the Commission's work. The NSCAI recognizes necessary changes will require considerable effort from the public and the private sector and hopes to begin building that momentum for change in the coming months.

Indeed, following release of the Final Report on March 12, 2021, Representative Stephen F. Lynch, Chairman of the House Subcommittee on National Security, held a joint hybrid hearing[2] with the House Committee on Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems about the Final Report's findings—over 100 recommendations and, of that total, more than 50 are related to the purview of the Armed Services Committee.

During the hearing, Dr. Eric Schmidt, Chairman of the NSCAI, provided a high-level overview of the 751-page Final Report. Chairman Schmidt explained that the first part of the NSCAI Final Report, "Defending America in the AI Era," focuses on implications of AI applications for defense and security. The second part, "Winning the Technology Competition," recommends the U.S. government take specific actions to promote and further AI innovation and national competitiveness, and to protect critical U.S. advantages in the larger strategic competition with China.

At the same time, the Final Report is also likely to increase scrutiny of the government's current use of AI. Indeed, the American Civil Liberties Union's recent decision to file a sweeping FOIA request[3] seeking information about how the government uses AI for national security, also seeks information about the risks such

technologies could pose to privacy and other individual rights. In this way, the Final Report's focus on privacy and civil liberties may presage increased interest and focus from public interest organizations, legislators and regulators in the months and years ahead.

Notes

* Katherine Sheriff is a technology associate at Davis Wright Tremaine LLP, devoting her legal practice to identifying areas of opportunity, and potential challenges, in emerging technology sectors, particularly in the dynamic fields of autonomous vehicles and artificial intelligence. K.C. Halm is a communications and technology partner at the firm and co-chair of its national multi-disciplinary AI practice group. Resident in the firm's Washington, D.C., office, the authors may be reached at katherinesheriff@dwt.com and kchalm@dwt.com, respectively.

1. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

2. https://oversight.house.gov/legislation/hearings/final-recommendations-of-the-national-security-commission-on-artificial.

3. https://www.aclu.org/aclu-foia-request-artificial-intelligence-national-security.