Opening Remarks
of
Jamil N. Jaffer[1]
on
The Role of Artificial Intelligence in Counterterrorism and Related National Security Programs and the Privacy and Civil Liberties Issues Associated with these Uses of Artificial Intelligence
before the
United States Privacy and Civil Liberties Oversight Board

July 11, 2024

I. Introduction

Chair Franklin and Members of the U.S. Privacy and Civil Liberties Oversight Board (PCLOB): thank you for inviting me here today to discuss the role of artificial intelligence (AI) in counterterrorism and related national security programs, and the privacy and civil liberties issues associated with these uses of AI.[2]

I want to thank Chair Franklin and the other members of the PCLOB for holding this forum in the context of the PCLOB's statutory responsibility to "analyze and review actions the executive branch takes to protect the Nation from terrorism…[and] ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."[3] This responsibility, focused specifically on the federal government's actions and efforts to protect the United States against the very real

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute (NSI) and the NSI Cyber and Tech Center (NSI CTC) and as an Assistant Professor of Law and Director of the National Security Law & Policy and Cyber, Intelligence and National Security Programs at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports, and invests in innovative companies that develop promising, early-stage technologies to address the critical cyber and advanced technological needs of both commercial and government customers, including companies in the cybersecurity, deep-tech, and artificial intelligence areas. Mr. Jaffer was also recently appointed to serve as a member of the Cyber Safety Review Board at the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Intelligence Committee, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice. Mr. Jaffer is speaking to United States Privacy and Civil Liberties Oversight Board in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or former employer. Mr. Jaffer would like to thank Devlin Birnie and Patrick Schmidt for their strong research assistance in support of these remarks.

[2] Portions of these remarks have been drawn in whole or in part from an NSI Decision Memo titled *Addressing the National Security Threat of Chinese Technological Innovation* by Mr. Jaffer published in July 2023, as well as from an op-ed written by Mr. Jaffer with former U.S. National Cyber Director Chris Inglis and Dr. Mary Aiken titled *As the U.S. Sprints Ahead on AI, Values Can't Be Left Behind*, published in Barron's in October 2023. Mr. Jaffer would like to thank Devlin Birnie, Jessica Jones, Harrison McClintock, and Alex Tokie for their excellent research and editing assistance with the NSI paper and his co-authors Chris Inglis and Dr. Mary Aiken for their collaboration on the op-ed. The original NSI paper can be found here and the Barron's op-ed can be found here.

[3] *See* 42 U.S.C. § 2000ee(c).

and ongoing threat of terrorism,[4] is particularly important today as we look at a world literally on fire.

From two major wars in the heart of Europe and the Middle East—one started by Russia invading another sovereign nation and the other kicked off by Hamas' brutal terrorist attack sponsored by the Iranian regime—it is hard to overstate the very real and pressing threats, including the direct threat of a terrorist attack in the United States or against American citizens abroad, that face our nation today.

Given this, it is truly an honor today to be appearing at this important event following a keynote address delivered by Senator Mike Rounds (R-SD), the co-chair of the Senate AI Caucus, member of the Bipartisan Senate AI Working Group, and a key leader on both the Senate Select Committee on Intelligence and the Senate Committee on Armed Services. It is likewise an honor to be here appearing on one of two panels alongside distinguished leaders and experts like Dr. Alondra Nelson, the former Acting Director of the White House Office of Science and Technology Policy, Justice Department Acting Chief Privacy and Civil Liberties Officer Peter Winn, the former Office of the Director of National Intelligence Chief Technology Advisor Dean Souleles, National Institute of Standards and Technology Senior Scientist Elham Tabassi, Special Competitive Studies Project Senior Intelligence Director Chip Usher, Center for Democracy and Technology AI Governance Lab Director Miranda Bogen, and National Association of Criminal Defense Lawyers Counsel Clare Garvie.

II. The Terrorist Threat Facing the United States

I'd like to start my brief remarks with a quick overview of the terrorist threat facing our nation today. Just last month, the Director of the Federal Bureau of Investigation (FBI) Christopher A. Wray told a Senate Appropriations Subcommittee that he was "hard pressed to think of a time when so many different threats to our public safety and national security were so elevated all at once" and specifically that "the threat from foreign terrorists [has] rise[n] to a whole 'nother level" since the October 7, 2023 terrorist attack by Hamas in Israel.[5] Director Wray went on to note that while "there was already a heightened risk of violence in the United States before October 7…[s]ince then, [the FBI has] seen a rogue's gallery of foreign terrorist organizations call for attacks against Americans and our allies," raising concerns not only that "individuals or small groups will draw twisted inspiration from the events in the Middle East to carry out attacks here at home" but also that there is "increasing[] concern[]…[about] the potential for a coordinated attack here in the homeland, akin to the ISIS-K attack we saw at the Russia Concert Hall in March."[6] That ISIS-K attack took the lives of nearly 150 and injured well over 500.

[4] *See, e.g.*, 42 U.S.C. § 2000ee(d)(1)-(2).

[5] *See* Federal Bureau of Investigation, *Director Wray's Opening Statement to the Senate Appropriations Committee Subcommittee on Commerce, Justice, Science, and Related Agencies: Remarks as Prepared for Delivery* (June 4, 2024), *available online at* < https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-senate-appropriations-committee-subcommittee-on-commerce-justice-science-and-related-agencies>.

[6] *Id*.

And Director Wray is not the only one flagging these concerns about terrorism here in the United States. One month ago, former FBI Deputy Director Michael Morrell and Harvard professor Graham Allison wrote in Foreign Affairs, in an article titled "The Terrorism Warning Lights Are Blinking Red Again" that "[p]ut simply, the United States faces a serious threat of a terrorist attack in the months ahead."[7] In support of this position, Morell and Allison not only cited Director Wray's testimony, but also highlighted the statements of CENTCOM Commander Gen. Erik Kurilla over the past couple of years about the growing capabilities al Qaeda, ISIS, and ISIS-K, and of Christine Abizaid, the outgoing director of the National Counterterrorism Center, who recently highlighted the growing terrorist threat environment, as well as the testimony of Attorney General Merrick Garland before the House Judiciary Committee in May 2024 where he noted that the threat level of a terrorist attack in the United States "has gone up enormously."[8]

The sources of these threats are diverse, but we know that the Iranian government and their terrorist proxy Hizballah both continue to obsess about the United States' killing of Qassem Soleimani, the leader of the Iranian Revolutionary Guards—Quds Force back in January 2020 and seek to plot their revenge, that ISIS and al Qaeda continue to have the intent to "carry out or inspire large-scale attacks in the United States," and specifically that ISIS "remains relentless in its campaign of violence against the United States and its partners— here at home and overseas."[9]

These threats are only heightened by the crisis at our southern border. Many of the experts and senior officials noted above, including Wray, Morrell, and Allison, have all noted that the porous nature of our southern border has caused foreign terrorists to seek to exploit this key vulnerability in recent months.[10] Indeed, articles and op-eds in newspapers as diverse as the New York Times and the New York Post have highlighted, in the last month alone, the illegal entry of Russians, Tajiks, and other foreign nationals with significant ties to terrorist groups through the southern border.[11]

[7] Michael Morrell & Graham Allison, *The Terrorism Warning Lights Are Blinking Red Again*, Foreign Affairs (June 10, 2024), *available online at* <https://www.foreignaffairs.com/united-states/terrorism-warning-lights-are-blinking-red-again>.

[8] *See id*.

[9] See Federal Bureau of Investigation, *Statement of Christopher A. Wray at a Hearing Entitled A Review of the President's Fiscal Year 2025 Budget Request for the Federal Bureau of Investigation* Senate Committee on Appropriations, Subcommittee on Commerce, Justice, Science and Related Agencies (June 4, 2024), at 4-5, *available online at* <https://www.appropriations.senate.gov/imo/media/doc/download_testimony80.pdf>.

[10] *See* Morrell & Allison, *Blinking Red*, supra n. 7.

[11] *See, e.g.*, Adam Goldman, Eric Schmitt & Hamed Aleaziz, *The Southern Border, Terrorism Fears and the Arrests of 8 Tajik Men*, New York Times (June 25, 2024), *available online at* <https://www.nytimes.com/2024/06/25/us/politics/terrorism-threat-fbi-tajik.html>; Editorial Board, *With Terror Threats Sky-High and the Border Wide Open, Brace for Another 9/11*, New York Post (June 11, 2024), *available online at* <https://nypost.com/2024/06/11/opinion/with-an-open-border-as-terror-threats-soar-brace-for-another-9-11/>.

While there are those who claim that this threat is overblown,[12] in my view, given the scope, nature, and consistency of these very stark warnings from a diverse and highly capable group of experts, it is critical that the federal government take immediate action to use all tools at our disposal to protect Americans at home and abroad from the threat of terrorism. Indeed, contrary to the advice provided by some,[13] I am of the view that if the federal government fails to take heed of these warnings and does not act now to utilize all aspects of modern technology available to us to protect our nation and its allies, including through the use artificial intelligence-enabled capabilities, we be putting the American people at increasingly greater peril.

III. Privacy and Civil Liberties Issues Arising from the Use of Artificial Intelligence in the Counterterrorism Context

In my view, the AI revolution is creating a virtually boundless set of opportunities and offers the potential to have a massively transformative effect writ large, serving as a tide that raises all boats, creating new innovation and capabilities, upskilling workers across a broad range of industries, and freeing innovators create even more productive tools and capabilities long into the future.[14] This is just as true in the counterterrorism and national security context as it is in other areas of government and private endeavors. And while there are very real, legitimate, and appropriate concerns being raised by certain critics about the potential for misuse of the data, tools, and capabilities used or enabled by AI, including particularly in the counterterrorism and national security context, the notion touted by some that AI could threaten our very existence or so deeply alter the balance of power in our society that it ought be treated like a dangerous pathogen or a nuclear weapon strikes me as deeply overwrought and lacking in substance.[15]

The potential for AI-enabled technology and tools to provide for significantly better collection on and identification and detection of actual terrorist threats is, without a doubt, massive. Given that both the keynote speech by Senator Rounds and the first panel have both spent a significant amount of time discussing the potential value that such capabilities can bring to our national security I will focus my brief remarks today on how we might ensure that these vast, new—and critically important—capabilities might be most rapidly and effectively deployed to protect the nation in a manner consistent with our core values, particularly given the current heightened terrorist threat environment that we face.

As we think about the issues raised by Senator Rounds and the first panel about how AI capabilities might enhance our ability to analyze signals and other intelligence gathered through a range of

[12] *See, e.g.*, Alex Nowrasteh and Michael J. Ard, *Alarmism about Terrorism Is Risky and Unjustified*, CATO Institute (July 2, 2024), *available online at* <https://www.cato.org/commentary/alarmism-about-terrorism-risky-unjustified>.

[13] *Id*.

[14] *See, e.g.*, Jamil N. Jaffer, *Addressing the National Security Threat of Chinese Technological Innovation*, National Security Institute (July 2023), at 7 & n. 79 (collecting sources), *available online at* <https://nationalsecurity.gmu.edu/wp-content/uploads/2023/08/The-National-Security-Threat-of-Chinese-Technological-Innovation.pdf>; Chris Inglis, Jamil N. Jaffer & Dr. Mary Aiken, *As the U.S. Sprints Ahead on AI, Values Can't Be Left Behind*, Barron's (Oct 26, 2023), *available online at* <https://www.barrons.com/articles/ai-regulation-nationalization-innovation-security-6d60ba33>.

[15] *Id*. (collecting sources).

sources from overhead imagery to human intelligence, there is good reason to step carefully—albeit not slowly—as we seek to ensure that we use these capabilities consistent with our values. This is important for a variety of reasons, including but not limited to the massive volume of data that we will be able to query, analyze, and otherwise utilize at scale given current and future advances in computing power and data storage, not to mention the rapid, ongoing advances in the AI tools themselves, including the large language models at the heart of the generative AI revolution. This data—even when collected under the full range of legal authorities provided to the federal government in the law enforcement and national security communities—can contain tremendous amounts of personal information, much of which may be sensitive and, particularly where it involves the information of non-consenting United States persons, may be protected under a range of domestic laws. Likewise, even where the data is not protected or is lawfully able to be accessed, stored, or analyzed, the nature of the data may often be such that access to or the inadvertent disclosure of the data—whether by mistake, theft, collection by an adversary, or intentional leak by a threat actor or malicious insider—could cause significant harm to an individual or group of Americans.

And, of course, it is not just the data itself, it is also the way these new tools and capabilities will allow us to analyze and use the data, including making predictive assessments about the actions, capabilities, plans, and intentions of suspected and known adversaries. In this context, as well as the many other analytic, assessment, and operational contexts that AI might be used in the counterterrorism enterprise as discussed by the keynote and the first panel, important questions about issues like predictive bias and unreliability (including but not limited to the so-called "hallucination" problem), to name just a few, are undoubtedly important and must be accounted for and addressed both when these capabilities are built and as they are deployed, including on a going-forward basis.

At the same time, given the very real and increasingly concerning threat environment we face today, it is crucial that we not unnecessarily or artificially slow down or limit our implementation of these capabilities in our counterterrorism enterprise out of fear that we might get it wrong. To do so, would, in my view, be a grave mistake.

Rather than artificially or unnecessarily limiting ourselves in the immediate deployment and roll out of these capabilities, the better approach may be to ensure—through work with the innovators, companies, organizations, and academics that are on the cutting edge of these innovations—that that the AI capabilities we deploy, including the models and algorithms themselves, as well as the compute hardware, software, and storage—are all built and deployed with trust, safety, and security baked in from the outset. Efforts like the development of secure-by-design and resilient-by-design principles being done cooperatively with industry by CISA and the development of frameworks along the lines of the NIST cybersecurity and AI risk management frameworks, based principally on rapidly developing and evolving private sector best practices, among other things, can help drive trust, safety, and security in the development of AI capabilities.

Likewise, the use the government's own buying power to set purchasing standards for the type of trust, safety, and security that needs to be built into government-bought capabilities can be a strong driver to protect not only data and capabilities used in the counterterrorism context but can also filter rapidly into the broader industry as well. And, of course, the government can effectively incentivize such efforts not only through its own buying power but also through the use of government incentives such as tax relief, access to research and development grant funding, and regulatory and liability relief as well. To be sure, there are those who would advocate for these use of more aggressive government regulation and disincentives like the creation of liability for software manufacturers and the like (i.e., the stick rather than the carrot) as a primary method for achieving these goals, but, in my view, given the difficulty of regulating rapidly evolving technologies and the significant negative effects such regulation could have on innovation, including significantly decreasing the velocity and scale of technology evolution (as our partners and allies in Europe oft experience), such an approach ought be limited only to the cases of clear market failures. And where, as here, you have well-understood challenges and broad recognition of the issues in play, as well as a rapidly expanding industry of trust, safety, and security tools that is increasingly being funded by capital allocators in the venture capital and broader finance communities,[16] there is no clear reason that the government ought reach for the regulatory stick now rather than trying the more innovation-friendly incentive approach and empowering private sector efforts to both invest in and build robust AI-focused trust, safety, and security capabilities.

Indeed, as noted above, a key and often overlooked set of players in creating effective trust, safety, and security capabilities and baking them into critically important AI tools being deployed in the counterterrorism context are the cutting-edge innovators in the early-stage startup space themselves and those that fund them. For example, Paladin Capital, (where I am a venture partner as noted in my bio above), in partnership with over a dozen prominent venture firms in the United States and Europe, including the NATO Innovation Fund, recently announced a set of Investment Principles and Commitments on Trust, Safety, and Security,[17] that commit these investors to investing in companies that put these issues, including the use of secure-by-design and resilient-by-design principles and the responsible use of AI, at the core of their companies' software design, development, and deployment processes. Likewise, these investment firms—many of whom invest in dual-use national security technologies—also voluntarily committed to investing in technology that supports the United States, NATO, and their allies, and to affirmatively not investing in companies that are building adversary capabilities or selling to adversary nations.[18]

These type of voluntary decisions, whether by capital allocators, innovators, or companies—who are making such choices not only because they believe in them as a moral, ethical, or patriotic matter but also because they represent good business choices—are exactly the kind of efforts that government ought embrace as the White House and NATO have done.[19] Indeed, such an approach, where private industry sees the benefit of investing in and building trusted, safe, and secure

[16] *See, e.g.*, Paladin Capital Group, PUBLIC & Perspective Economics, *International State of Safety Tech 2023* (Dec. 6, 2023), *available online at* <https://view.publitas.com/public-1/international-state-of-safety-tech-report-2023/page/1>; Duco Experts Group, *Trust and Safety Market Research Report* (Mar. 13, 2024), *available online at* <https://duco-public-static-assets.s3.amazonaws.com/Duco+TnS+MRR-+FINAL.pdf>.

[17] *See* Paladin Capital Group, et. al, *Investment Principles and Commitments on Trust, Safety, and Security* (2024), available online at <https://www.paladincapgroup.com/investment-principles-and-commitments/>.

[18] *Id*.

[19] *See* Paladin Capital Group, *Paladin Capital Group Announces Additional Signatories to Investment Principles & Commitments to Defend International Security and Promote Innovation* (Jul 8, 2024), *available online at* <https://www.paladincapgroup.com/paladin-capital-group-announces-additional-signatories-to-investment-principles-commitments-to-defend-international-security-and-promote-innovation/>.

technologies because it will enhance uptake of new technologies, ensure that users both on an individual and commercial scale obtain the benefits of the baked-in security, and protect the intellectual property of innovative companies for whom such IP is the lifeblood of the enterprise, and therefore are able to take advantage of the better return profiles that come from such investments, may be one key method for gaining traction in these areas.

It is also worth noting that major technology innovations as applied in the national security context—while sometimes initially seen as concerning from a privacy and civil liberties perspective—often can play out in ways that can be privacy-promoting and enhancing. For example, while many expressed a broad range of concerns about the use of large-scale metadata collection and analysis conducted under Section 215 program, that program was ultimately authorized by statute in the USA Freedom Act—albeit subject to specific limitations—based in part on a recognition that the use of metadata to identify potentially new and unknown targets and to eliminate the need to conduct full content collection on potentially relevant targets can provide significant value. While that program was ultimately discontinued—and certain of the underlying authorities remain expired—the notion of the use of metadata collection as an alternative to other, more intrusive collections is one that may also be usefully applied to the AI context as well. Likewise, one might look at other advanced technologies, such as the use of drones and highly precise, customizable weapons payloads in counterterrorism operations, which while raising a range of moral and ethical concerns in the early days (and for some even today), have nonetheless provided significant value and significantly reduced potential harm to non-combatants in many counterterrorism operations. And while the analogies in this space are, of course, significantly more remote when applied to the current group of AI-enabled counterterrorism applications, it is worth noting that technology innovation can—and often does—play a positive role, and one that is consistent with our core values.

Finally, as we think about the use of AI in the counterterrorism context, it is also worth noting that there are some areas of clear consensus in related areas that could inform our views on how AI ought be deployed here. For example, it is widely accepted in the U.S. that the use of lethal force should not be delegated to fully automated systems. That is, the Department of Defense's long-standing—and current—position is that a human must be "in-the-loop" and must make the final call when lethal force is used against another person, even when technology augments that decision-making.[20] Given this consensus, we could imagine a world in which in counterterrorism analytic or decisionmaking contexts where we applied a similar requirement, or perhaps a "human-on-the-loop" approach where a human may not be required to decide on an automated or AI-enabled action, but may be able to limit its use, impact or scope once underway.

Such approach may seem obvious, and accord well with our values, but this is a place where, if we are to be truly as effective as possible, policymakers need to provide clear guidance on the roles they expect—and require—human decisionmakers to play in counterterrorism analysis or operations enabled by AI.

[20] *See* Inglis, et. al, *As the U.S. Sprints Ahead on AI*, *supra* n. 14.

IV. Conclusion

At the end of the day, what can be certain about the application of AI in the counterterrorism context is that building in trust, safety, and security from the outset in these capabilities is critical. This is because, without doing so, there is a significant chance that we will not see the adoption necessary to take advantage of what could be a transformative capability with the potential to drastically enhance our defensive capabilities at time of great need. As such, we ought lean forward on the adoption of these technologies, while doing so consistent with our values and taking strong path forward on both the immediate and effective—and privacy protective—use of these capabilities in the American counterterrorism enterprise.