July 11, 2024

Opening Statement from Clare Garvie
Training & Resource Counsel, Fourth Amendment Center
National Association of Criminal Defense Lawyers (NACDL)

Before the Privacy and Civil Liberties Oversight Board (PCLOB)
Public Forum on the Role of AI in Counterterrorism and Related National Security Programs

Dear Chair Franklin, and Board Members Felten, LeBlanc, and Williams, thank you for the opportunity to speak with you today.

Ten years ago, an Israeli company called Faception began marketing an AI-based system to identify possible future terrorists, in real-time, without any prior intelligence on the person required. The tool, according to the start-up, could predict someone's propensity to be involved in future acts of violence based on an analysis of their facial features, captured at a distance.[1]

When asked by a Wall Street Journal reporter about the foundational validity—or reliability—underpinning this tool, Shai Gilboa, co-founder and CEO of Faception stated: "I need to emphasize that there is no scientific evidence for the terrorist classifier."[2]

Nonetheless, the system continues to be promoted, and is in use by at least two — as of yet unnamed — countries' defense agencies.[3] The company also markets tools to identify possible white-collar criminals, pedophiles, brand promoters, bingo players, and academic researchers.[4]

---

[1] About Us, Faception, https://www.faception.com/about-us (*last accessed* July 10, 2024).
[2] Hilke Schellmann, *Weighing the Costs and Benefits of Facial Recognition Technology*, Wall Street Journal (Nov. 19, 2018), https://www.wsj.com/articles/facial-recognition-goes-mainstream-drawing-concerns-1542623401.
[3] *Id*.
[4] Our Classifiers, Faception, https://www.faception.com/our-technology (*last accessed* July 10, 2024).

I highlight this tool not because I suspect the U.S. is one of the countries using it (I have no evidence one way or the other), but because it illustrates many of the privacy, civil liberties, reliability, transparency and other concerns with AI that we're here to discuss today, including:

1. The often-unquestioned impulse to see AI as providing a solution to all intelligence, national security, and law enforcement challenges — the ability to identify the next potential plot, screen travelers, gather evidence — without considering the true costs or considering viable alternatives.
2. The fact that AI may over-promise and under-deliver. Put simply, we risk deploying junk science in an extremely high-consequence environment, both for national security and the people investigated or denied access or benefits based on AI determinations.
3. The threat of entrenching existing, often biased, heuristics about what or who constitutes a threat. Faception's "terrorist" classifier appears to look for Middle Eastern male facial features,[5] failed to flag Ted Kaczynski as a possible threat, and at least initially wasn't trained on women at all.[6] This bias is well documented across facial recognition deployments but is in no way unique to facial recognition alone.
4. The increasing reliance on AI to define and identify what constitutes anomalous, or suspicious, people or behaviors, risking supplanting human and judicial determinations of probable cause, and in some cases, guilt.
5. The tendency for AI systems to add layers of opacity into already deeply nontransparent sectors like intelligence and national security.

As this Board is of course very aware, two of the core mechanisms to ensure privacy and civil liberties in the intelligence and national security space are: (1) the minimization of collection, retention, and dissemination of U.S. persons' data; and (2) transparency and oversight.[7]

---

[5] *See* Detecting Potential Offenders in Faception Pitch (June 8, 2016), *available at* https://www.youtube.com/watch?v=x1QsDiWCV-o (0:57 of 2:02).
[6] *Supra* note 2.
[7] This is highlighted in the Final Report of the National Security Commission on Artificial Intelligence (NSCAI), which noted that "core features of [the American system] include laws, rules, and procedures to minimize the

In evaluating the national security applications of artificial intelligence, I urge Board to consider that AI, and the promise it holds out, is in tension to these mechanisms. Many AI systems promote the ability to ingest and make sense of vast quantities of disparate information about people, associations, behaviors, and more. This, combined with system needs for large, representative training datasets, creates an incentive for *more* — not less — data collection, retention, and dissemination. On transparency and oversight, the black box nature of algorithms, coupled with the trade secret claims that accompany private-sector development of algorithms, often leave the agency users themselves — not to mention the public — uninformed of potential sources of error and bias, and threats to privacy and civil liberties. This is exacerbated by the rapidly evolving nature of AI-based systems, a pace that our current structure of Privacy Impact Assessments and Systems of Records Notices has little hope of keeping up with.

In evaluating the national security applications of AI, I urge the Board to orient first and foremost to the question of whether it is necessary that a given tool be AI-based at all, or whether the data collection, opacity, reliability, or bias harms posed by the system outweigh the purported benefits. I also encourage the Board to push the intelligence and national security community to think critically about whether the current oversight and transparency structure is adequately responsive to the realities of AI, and its pace of development and deployment, in the face of those harms.

Thank you so much. I look forward to your questions.

collection, retention, and dissemination of U.S. persons' data, as well as oversight from all three branches of government." Final Report, p. 144, NSCAI (March 2021), https://reports.nscai.gov/final-report/.