ARTIFICIAL INTELLIGENCE AND CRIMINAL EXPLOITATION: A NEW ERA OF RISK

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

WEDNESDAY, JULY 16, 2025

Serial No. 119–31

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

61–182 WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California
ANDY BIGGS, Arizona
TOM MCCLINTOCK, California
THOMAS P. TIFFANY, Wisconsin
THOMAS MASSIE, Kentucky
CHIP ROY, Texas
SCOTT FITZGERALD, Wisconsin
BEN CLINE, Virginia
LANCE GOODEN, Texas
JEFFERSON VAN DREW, New Jersey
TROY E. NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
HARRIET M. HAGEMAN, Wyoming
LAUREL M. LEE, Florida
WESLEY HUNT, Texas
RUSSELL FRY, South Carolina
GLENN GROTHMAN, Wisconsin
BRAD KNOTT, North Carolina
MARK HARRIS, North Carolina
ROBERT F. ONDER, JR., Missouri
DEREK SCHMIDT, Kansas
BRANDON GILL, Texas
MICHAEL BAUMGARTNER, Washington

JAMIE RASKIN, Maryland, *Ranking Member*
JERROLD NADLER, New York
ZOE LOFGREN, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
ERIC SWALWELL, California
TED LIEU, California
PRAMILA JAYAPAL, Washington
J. LUIS CORREA, California
MARY GAY SCANLON, Pennsylvania
JOE NEGUSE, Colorado
LUCY MCBATH, Georgia
DEBORAH K. ROSS, North Carolina
BECCA BALINT, Vermont
JESÚS G. "CHUY" GARCÍA, Illinois
SYDNEY KAMLAGER-DOVE, California
JARED MOSKOWITZ, Florida
DANIEL S. GOLDMAN, New York
JASMINE CROCKETT, Texas

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

ANDY BIGGS, Arizona, *Chair*

TOM TIFFANY, Wisconsin
TROY NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
LAUREL LEE, Florida
BRAD KNOTT, North Carolina

LUCY MCBATH, Georgia, *Ranking Member*
JARED MOSKOWITZ, Florida
DAN GOLDMAN, New York
STEVE COHEN, Tennessee
ERIC SWALWELL, California

CHRISTOPHER HIXON, *Majority Staff Director*
JULIE TAGEN, *Minority Staff Director*

C O N T E N T S

WEDNESDAY, JULY 16, 2025

OPENING STATEMENTS

Page

The Honorable Andy Biggs, Chair of the Subcommittee on Crime and Federal Government Surveillance from the State of Arizona 1
The Honorable Lucy McBath, Ranking Member of the Subcommittee on Crime and Federal Government Surveillance from the State of Georgia 3

WITNESSES

Dr. Andrew S. Bowne, Professor, George Washington University
Oral Testimony 5
Prepared Testimony 8
Zara Perumal, Chief Technology Officer, Overwatch Data
Oral Testimony 24
Prepared Testimony 26
Cody Venzke, Senior Policy Counsel, National Political Advocacy Division, American Civil Liberties Union
Oral Testimony 40
Prepared Testimony 42
Ari Redbord, Global Head of Policy, TRM Labs
Oral Testimony 72
Prepared Testimony 74

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

All materials submitted by the Subcommittee on Crime and Federal Government Surveillance, for the record 104

Materials submitted by the Honorable Lucy McBath, a Member of the Committee on the Judiciary from the State of Georgia, for the record
- A letter to Speaker Mike Johnson, Minority Leader Hakeem Jeffries, Majority Leader John Thune, and Minority Leader Chuck Schumer, from the National Association of Attorneys General, May 16, 2025
- An article entitled, "Inside Congress Live," Jun. 27, 2025, *Politico*
- A testimony from Barry Friedman, Jacob D. Fuchsberg Professor of Law and Affiliated Professor of Politics, Faculty Director, Policing Project, New York University School of Law, Jul. 16, 2025
- A letter to the Honorable Andy Biggs, Chair of the Subcommittee on Crime and Federal Government Surveillance from the State of Arizona, and the Honorable Lucy McBath, Ranking Member of the Subcommittee on Crime and Federal Government Surveillance from the State of Georgia, from PublicCitizen, Jul. 16, 2025
- A testimony from Keith Kupferschmid, Chief Executive Officer, Copyright Alliance, Jul. 16, 2025

Page

An article entitled, "The countdown to artificial superintelligence begins: Grok 4 just took us several steps closer to the point of no return," Jul. 12, 2025, *The Blaze*, submitted by the Honorable Andy Biggs, Chair of the Subcommittee on Crime and Federal Government Surveillance from the State of Arizona, for the record

APPENDIX

A statement from the Honorable Jamie Raskin, Ranking Member of the Committee on the Judiciary from the State of Maryland, Jul. 16, 2025, for the record

ARTIFICIAL INTELLIGENCE AND CRIMINAL EXPLOITATION: A NEW ERA OF RISK

Wednesday, July 16, 2025

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

COMMITTEE ON THE JUDICIARY

Washington, DC

The Subcommittee met, pursuant to notice, at 10 a.m., in Room 2141, Rayburn House Office Building, the Hon. Andy Biggs [Chair of the Subcommittee] presiding.

Members present: Representatives Biggs, Kiley, Lee, Knott, and McBath.

Also present: Representative Raskin.

Mr. BIGGS. The Subcommittee will come to order. Without objection, the Chair is authorized to declare a recess at any time. We welcome everyone to today's hearing on Artificial Intelligence and Criminal Exploitation.

I now recognize the gentlewoman from Florida, Ms. Lee, to lead us in the Pledge of Allegiance.

ALL. I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation, under God, indivisible, with liberty and justice for all.

Mr. BIGGS. Thank you. I now recognize myself for an opening statement. I appreciate everyone being here today, our witnesses, and those in the audience. This is an important hearing which focuses on artificial intelligence and how it is being exploited by criminals. The conceptual roots of AI can be traced to British mathematician Alan Turing when the 1930s theorized about a machine being capable of performing any computable task. Today, AI is best understood as a branch of computer science that leverages large scale data processing, algorithmic modeling, and modern hardware to enable machines to perform tasks typically requiring human cognition.

Unfortunately, like most technical innovations, the criminal element has begun to use AI to enhance their elicit activities. The AI-enabled threats continue to evolve as bad actors use AI technology in a wide spectrum of criminal enterprises. From deepfake scams and synthetic identity fraud to financial crimes and child sexual abuse material, CSAM, the landscape continues to evolve at a rapid

pace as AI provides users with enhanced capabilities. The AI-based or AI-driven threats and schemes can cost businesses millions of dollars a year including both prevention and falling prey to them. In one case, fraudsters used AI to clone a CEO's voice and authorized a wire transfer. Among corporations that experienced a rise in deepfake incidents, 75 percent of deepfakes impersonated a CEO or another C suite executive.

Generative AI enables the criminal exploitation of victims' emotional vulnerabilities through tactics such as sextortion, pig-butchering scams, phishing, and elder fraud. Senior citizens are increasingly targeted through voice phishing scams where an AI-generated replica of a grandchild or military officer claims to need urgent funds. In one case, a Colorado mother received a call from what sounded like her daughter pleading for help. The voice was AI generated, closed from a short, online clip and used to demand ransom. The voice was indiscernible to the mother who wired $1,000 to scammers in Mexico.

AI is also fueling a rise in sextortion and synthetic CSAM. New AI tools can generate highly realistic, but entirely fabricated explicit images often used to extort minors or damage reputations. Some sextortion scams exploit the trust associated with platforms like Apple's iMessage by impersonating classmates or romantic interests via recognizable blue bubble interfaces. Criminals now deploy apps like Muah to fabricate child abuse images at scale. Stanford University researchers have uncovered evidence that generative models were trained on real exploitative content.

Terrorist groups now utilize AI to target, recruit, and indoctrinate vulnerable individuals. Generative AI provides a degree of separation, allowing actual terrorists to maintain anonymity in their public facing recruiting practices. Generative AI also allows terrorists to produce propaganda, fake news stories, and emotionally resonant messages tailored to specific psychological profiles.

Reports of generative artificial intelligence enabled scams between May 2024–May 2025 rose by 456 percent. The use of exploitive generative AI allows criminals to produce human-like text, code, images, and videos allowing criminals to use the technology for further criminal activity such as creating more realistic phishing lures or generating deepfakes for extortion.

On average, phishing attacks cost $4.9 million per breach. On the other hand, AI is increasingly integrated into police investigations offering new tools and capabilities for law enforcement agencies into the backdrop of rapidly expanding digital data sources and increasing demands on law enforcement agencies. AI provides a more adaptable and comprehensible approach to solving crimes, compared to traditional methods leveraging data analytics, machine learning, and pattern recognition to enhance investigations and assist with administrative tasks. This is also potentially a problem, as well, as we seek to balance curbing AI with our civil rights.

AI can also help process large volumes of data, identify patterns, and generate actionable insights, and in turn, these applications can improve efficiency, accuracy, and resource allocation with investigative processes. However, to fully benefit from AI applications, law enforcement entities need reliable data, human over-

sight, while also tackling issues related to privacy, bias, and ethical considerations. Addressing the continued misuse of AI will require a varied approach while also raising public awareness about the risks associated with AI-generated content.

Law enforcement agencies must engage openly with community stakeholders, legal experts, and the public to communicate the intended uses, benefits, and limitations of AI technologies. The collaborative effort to both prevents the misuse of AI while encouraging lawful application is required to effectively navigate this evolving landscape.

I am excited about today's hearing. I think this is the first of its kind. I believe it will be only the first of its kind as we consider AI and its continued expansion of influence on our lives. I am looking for a very substantive discussion—I anticipate a substantive discussion that we are going to have today and with that, I yield back and recognize now our Ranking Member, Ms. McBath, for her opening statement.

Ms. MCBATH. Well, thank you so much, Mr. Chair, and thank you to our witnesses today. Thank you so much for taking moments out of your day to come before us. Thank you for convening this hearing to discuss AI-enabled crime, efforts to detect and combat such crime, and how law enforcement deploys AI tools.

Like so many new technologies, AI is not inherently good or bad. The AI-enabled tools can find patterns, sort through vast amounts of information, and may even help law enforcement solve their crimes. In the wrong hands, the same tools can be used to commit financial fraud, breach national security systems, and to harm our children. When used by law enforcement, this technology has the potential to empower our investigators, while also carrying the risk of serious errors with life-changing consequences. That is why it is critical that we proceed thoughtfully and put appropriate guardrails in place so that everyone in our criminal justice system that is using AI-enabled tools, they are using them responsibly, not to the detriment of law-abiding members of our community.

You have already seen what can go wrong when those safeguards are missing. A woman and her family experienced the dangers of using AI enabled facial recognition technology. Detroit police used a facial recognition tool in an attempt to identify a carjacking suspect using an image from a surveillance camera. The tool matched the surveillance image with a picture of Porcha Woodruff, a nursing school student. One morning, as Ms. Woodruff was getting her two children ready for school, the police knocked on her door and they told her that she was under arrest for carjacking. She knew right away there must be some kind of mistake, and she gestured at her body as she spoke to law enforcement to point out the obvious, she hoped, to law enforcement that she was eight months pregnant. Though the police had not been looking for a visibly pregnant woman, they still handcuffed Ms. Woodruff, took her away from her crying children, held her for 11 hours, searched her phone, and they charged her. After her release, she went straight to the hospital and was treated for dehydration. The charges were dismissed a month later.

This case is especially troubling because facial recognition tools have been shown to perform worse on Black individuals, increasing

the risk of misidentification and contributing to over criminalization. AI is only as good as the data is it trained on and when that data is biased, it exacerbates racial disparity, long embedded in our criminal justice system, and an inaccurate tool is dangerous for every single one of us. Not one of us is immune to these mistakes.

Thankfully, and in due part to cases like this one, the city of Detroit has adopted new rules to direct the use of facial recognition technology within its police department, and they are simply not alone. Many cities and states have put sensible guardrails in place to limit potentially harmful uses of AI. That is why it was alarming when some of my Republican colleagues recently attempted to pass a moratorium on State and local AI regulations in the big ugly bill, a move that generated bipartisan opposition so much that 40 State Attorney Generals and 17 Republican Governors, including the Governor of my State, Georgia, wrote letters to the Senate in opposition to the proposed moratorium. The Governors warned that, and I am quoting them, "People will be at risk until basic rules ensuring safety and fairness can go into effect."

As you will see behind me, Sarah Huckabee Sanders, the Republican Governor of Arkansas and former press secretary to President Trump, took to Twitter to quote,

> I stand with the Majority of GOP Governors against stripping States of the right to protect our people from the worst abuses of AI. The U.S. must win the fight against China on AI and everything else, but we won't if we sacrifice the health, safety, and prosperity of our people.

While this most recent proposal was ultimately stripped from the bill by a 99 to one vote of the Senate, the Republican Chair of the House Energy and Commerce Committee has already vowed to continue to pursue a moratorium, even while acknowledging that Federal regulations on AI are still light years away.

I stand with those seeking to protect the health and the safety and civil rights of our communities from the abuses of AI and I hope that we can come together and follow the lead of the States to explore what those guardrails should look like and put them in place.

I look forward to learning more from our experts here today. Hearing from you is going to be extremely critical for us on this very important issue.

Before I yield, Mr. Chair, I ask unanimous consent to enter into the record two letters. The first is a letter from 17 Republican Governors in opposition to a moratorium on State and local regulation on AI; and the second, a letter from 40 State Attorneys General, both Republicans and Democrats, in opposition to a moratorium on State and local regulation of AI.

Mr. BIGGS. Without objection.

Ms. MCBATH. I yield.

Mr. BIGGS. The gentlelady yields. Without objection, all other opening statements will be included in the record. We will now introduce today's witnesses, and we are very grateful for our witnesses.

Dr. Andrew Bowne.

Dr. BOWNE. Bowne.

Mr. BIGGS. Bowne, OK. Dr. Bowne is a Professorial Lecturer in Law at the George Washington University Law School where he

teaches courses on artificial intelligence law and policy. He has served in the United States Air Force Judge Advocate General Corps since 2010 and previously serves as the Chief Legal Counsel of the Department of the Air Force Artificial Intelligence Accelerator at the Massachusetts Institute of Technology.

Thank you, Doctor, for being with us today.

Ms. Zara Perumal is the Co-Founder and Chief Technology Officer of Overwatch Data, an artificial intelligence company focused on threat intelligence and cybercrime tactics on the dark web. Prior to founding Overwatch Data, she worked at Google on matters involving machine learning and cyber security threats.

Thank you for you being us today, Ms. Perumal.

Mr. Ari Redbord is the Global Head of Policy at TRM Labs, a company focused on preventing illicit financial activity. He previously served as Senior Advisor to the Deputy Secretary and Under Secretary for Terrorism and Financial Intelligence at the U.S. Treasury. Prior to Treasury, he was an Assistant U.S. Attorney where he focused on terrorism, espionage, financial, child exploitation, and human trafficking cases.

Thank you, Mr. Redbord, for being with us today.

Mr. Cody Venzke is a Senior Policy Counsel in ACLU's National Political Advocacy Department where his work focuses on surveillance, privacy, and technology. Specifically, he works on matters related to artificial intelligence, privacy, children's privacy, and civic uses of data.

Thanks, Mr. Venzke, for being with us today.

We appreciate all of you being here and now ask that you please rise so you can be sworn in.

Would you please raise your right hand? Do you swear or affirm under penalty of perjury that the testimony that you are about to give is true and correct to the best of your knowledge, information, and belief so help you God?

Let the record reflect the witnesses have answered in the affirmative and thank you, you may be seated. Please know that your written testimony will be entered into the record in its entirety. Accordingly, we ask that your testimony be summarized in five minutes and what is going to happen, just so you know, is about 15 seconds before the end, you will start hearing this, something like that, and then at the magic moment, I will start getting a little bit louder, but it will kind of help you wrap up on time, so we can work this out. We are so grateful that you are here.

Mr. Bowne, you may begin with your five minutes.

STATEMENT OF ANDREW S. BOWNE

Dr. BOWNE. Thank you, Mr. Chair, Ranking Member, and the distinguished Members of the Subcommittee. Thank you for the opportunity to testify to the intersection of artificial intelligence and criminal exploitation.

My name is Andrew Bowne. I serve as a Professorial Lecturer at the George Washington University Law School where I teach courses on AI law and policy. I have served in the United States Air Force Judge Advocate Generals Corps since 2010 including assignments as a prosecutor, a staff Judge Advocate General Counsel

Air Force installation, and as you heard, a Chief Legal Counsel for the Air Force's AI Accelerator at MIT.

I do appear today in my personal capacity. The views I present are my own and do not necessarily reflect those of the Department of Defense, the Department of the Air Force, or the Judge Advocate Generals Corps.

AI is both a catalyzing and transformative technology enabler, a solver of traditional processes, but also creates entirely new ones. When a task AI is used for is criminal or harmful, the nature of AI becomes a threat multiplier. The AI systems now automate decisions, model environments, and infer actions of unprecedented speed, and scale. While they are designed to benefit society, their dual-use nature means they could also facilitate exploitation, fraud, and abuse. Even AI systems designed with legitimate use in mind can create harm if not carefully designed and deployed with safety, ethics, and accountability built in.

Today, I would like to briefly highlight how AI enables criminal activity, the gaps in current criminal law, and proactive steps Congress might take. First, how AI enables criminal activity. I am seeing really three categories of AI developments that are of particular concern in this area: Computer vision, generative adversarial networks, or GANS, and large language models, or LLMS.

Computer vision systems which interpret visual data are used to automate surveillance, identify targets, and even harvest personal data from breached documents for identity threat and fraud or enable real time threat detection for public safety that can be repurposed to stalk or blackmail individuals with chilling efficiency. GANs are capable of generating synthetic images, videos, and audio that are known in public discourse as deepfakes. These tools allow the impersonation of public officials and private citizens alike. Multiple watchdogs and law enforcement agencies that have been conducted longitudinal analysis on AI generated child sexual abuse material or CSAM are reporting rapid rises in the number of generated images shared online. Perhaps more concerning is that the increased capabilities of sophistication of generative AI models enable them to produce very realistic images.

Generative AI tools are also used for sextortion, grooming, and emotional coercion, often targeting children. Large language models like those powering chatbots revolutionizing phishing, fraud, and social engineering involve misinformation. They engage victims and extend realistic conversations, target elderly people and vulnerable people in scams or overwhelming financial institutions of thousands of tailored loan applications. They are also used to generate malicious code, making cybercrime accessible to individuals with no technical background. In short, deepfakes, AI generated CSAM, and automated fraud are not theoretical threats. They are real, growing, and causing harm now. The barrier to entry to using AI to perpetuate or perpetrate is low. Anyone with a few seconds of your voice or image can create convincing synthetic content without coding or expensive hardware. The tools are cheap, accessible, and often unregulated.

Tragically, gaps in current Federal criminal law allow bad actors to use AI to profit at the expense of others, prey on the vulnerable or create mistrust with impunity. While there are statutes for wire

fraud and child sexual abuse material, they do apply to many of the AI-enabled crimes, there are several significant gaps.

More alarming still are emerging threats such as autonomous criminal activity, cross-board AI enabled crime, and algorithmic market manipulation in which criminal liability is unclear or altogether absent.

There are a variety of strategies that the Committee, as well as Congress, can consider, including criminal law reform. They could define new offenses from malicious use of AI, particularly deepfakes and AI CSAM. They could also provide sentencing enhancements for crimes aggravated by the use of AI tools when those tools augment the scale or impact of the harm or make it more resource intensive to investigate and prosecute.

You could also look at enabling AI safety and transparency requirements and in conclusion AI is a revolutionary enabler but does not self-regulate. The bad actors who choose to exploit the law must be ready. Thank you, Mr. Chair, for the time.

[The prepared statement of Mr. Bowne follows:]

Testimony for
Subcommittee on Crime and Federal Government Surveillance
Committee on the Judiciary
U.S. House of Representatives

Hearing on "Artificial Intelligence and Criminal Exploitation: A New Era of Risk"
July 16, 2025

Andrew S. Bowne, PhD, JD, LLM
Professorial Lecturer of Law, The George Washington University Law School
United States Air Force Judge Advocate
Former Chief Legal Counsel, Department of the Air Force Artificial Intelligence Accelerator at the Massachusetts Institute of Technology

Disclaimer: The views presented in this testimony are those of the speaker and do not necessarily represent the views of DoD, Department of the Air Force, or the Air Force Judge Advocate General.

Testimony for
Subcommittee on Crime and Federal Government Surveillance
Committee on the Judiciary
U.S. House of Representatives

Hearing on "Artificial Intelligence and Criminal Exploitation: A New Era of Risk"
July 16, 2025

Mr. Chairman and distinguished members of the Committee: thank you very much for the opportunity to testify today on the critical intersection of artificial intelligence and criminal law. My name is Andrew Bowne, and I am a professorial lecturer in law at the George Washington University Law School, where I teach courses on AI, law, and policy. Previously, I was a professor of contract law and national security law at The Judge Advocate General's School, where I created courses focused on emerging technology. I hold a Ph.D. from the University of Adelaide in law and AI, an LL.M. focused on contract and fiscal law from the Judge Advocate General's School, a J.D. from the George Washington University, a B.A. in political science from Pepperdine University, and am a graduate of various Air Force and joint service schools. I am currently a candidate for a master's degree in International Public Policy at the Johns Hopkins University School of Advanced International Studies, as a member of the U.S. Space Force's *West Space Scholars* program. I have served as an active-duty judge advocate in the United States Air Force since 2010. In this role, I have been assigned as a prosecutor, staff judge advocate, and deputy staff judge advocate, deployed rule of law advisor, as well as the chief legal counsel and researcher at the Department of the Air Force's Artificial Intelligence Accelerator at the Massachusetts Institute of Technology. I am here today, speaking in my personal capacity as a scholar specializing in the intersection of AI and law, particularly as it impacts our national security. The views presented are my own and do not necessarily reflect the views of the Department of Defense or any of its components.

Introduction

Artificial intelligence is both a catalyzing and a transformative technology enabler. It is catalyzing in that it has accelerated and made more intense longstanding systems and constructs, and transformative in how it changes the nature of those systems and constructs into entirely new, scaled-up versions.[1] This is true for the accomplishment of any task aided by AI systems; it is also true when that task is criminal or harmful.

Defined in 15 U.S.C. § 9401, artificial intelligence is a machine-based system that can, for a given set of human-defined objectives, make *predictions, recommendations, or decisions* influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to:

(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and

[1] See Insights, MIT Technology Review, *Battling Next-Gen Financial Fraud* (quoting John Pitts, global head of industry relations and digital trust for Plaid).

(C) use model inference to formulate options for information or action.

With the confluence of advancements in machine learning algorithms, voluminous AI-ready data, and fast and inexpensive compute power, AI has transitioned from the realm of science projects or science fiction to household utility, digital agent, and enabler of a new wave of technological revolution. While the vast resources dedicated to the advancement of AI are intended to advance society, the nature of AI makes it inherently dual-use. Models developed to detect cancer from images can be used to create realistic fake images. Large language models that can help increase business system efficiencies and aid in communication can be used to spread misinformation and promote malicious social engineering. Even tools that can assist law enforcement and protect public safety can be used to stalk, target, and exploit victims and even escape detection. Thus, the safety and social utility of AI systems depend on how they are used. However, even if developed with legitimate use in mind, AI systems can create harm if not carefully designed and deployed with safety and ethics grounded in the system and responsibly used by the operator. AI systems that autonomously drive vehicles can, and have, resulted in deadly consequences,[2] and AI-generated sexual imagery and child pornography have created unprecedented ways to proliferate child sexual abuse material (CSAM).[3] "Virtually all activity involves a risk of harm, and as AI comes to do more, it will inevitably cause more harm."[4] My testimony is aimed at informing this committee on how AI technologies enable criminal and harmful activity through three common AI-enabled capabilities, gaps in criminal law, and recommended steps to address AI-enabled harms.

I. How AI Technologies Enable Criminal Activity

Artificial intelligence has fundamentally altered the criminal landscape by providing bad actors with sophisticated tools that amplify traditional crimes and enable entirely new categories of harmful conduct. Three core AI technologies—computer vision, generative adversarial networks (GANs), and large language models (LLMs)—have become particularly potent weapons in the criminal arsenal.

A. Computer Vision: The Eyes of Digital Crime

Computer vision systems, which analyze and interpret visual information, have enabled actors to conduct surveillance, identify targets, and automate activities at an unprecedented scale.[5] The capability created by these models can be used to find, track, surveil, and potentially harass,

---

[2] Mark MacCarthy, *The evolving safety and policy challenges of self-driving cars*. (July 31, 2024). Brookings. https://www.brookings.edu/articles/the-evolving-safety-and-policy-challenges-of-self-driving-cars/.

[3] Madisen Campbell, *Guardians of Innocence: Safeguarding Children in the Digital Age by Addressing the Legal Implications of AI-Generated Sexually Explicit Content*, XI-I Georgetown Univ. Undergraduate L. Rev. 25, 29 (2025).

[4] Ryan Abbott & Alex Sarch, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, 53-1 UC Davis L. Rev. 323, 330 (2019).

[5] See Kalluri, P.R., Agnew, W., Cheng, M. *et al.* Computer-vision research powers surveillance technology. *Nature* 643, 73–79 (2025).

stalk, kidnap, or otherwise harm someone. Facial recognition software can be used to identify high-net-worth individuals from social media photos, subsequently targeting them for scams or blackmail. When a computer vision model can process thousands of images daily, it can create detailed profiles of potential victims based on visual cues about wealth and lifestyle. Criminal networks can employ these systems to sort through vast databases of illegal imagery automatically, tagging content by age, location, and other characteristics to facilitate distribution and monetization.

Computer vision can also enable identity theft operations. These models can instantly analyze driver's licenses, passports, and other documents captured through data breaches, automatically extracting personal information and generating synthetic identities. This data is a gold mine for facilitating identity theft.

Essentially, good data collection and processing practices that data scientists use to ensure AI systems complete desired tasks are also leveraged by bad actors to increase effectiveness in illicit activities.

B. Generative Adversarial Networks: Manufacturing Deception

Generative AI algorithms are a type of AI algorithm that is used to generate novel data samples used to create a variety of media and have found applications in art, imaging, engineering, protein folding, and modeling.[6] Generative Adversarial Networks (GANs), which entail two neural networks, a "generator" and "discriminator", pitted against each other to generate increasingly realistic synthetic content, have become the foundation for a new generation of fraud and exploitation.[7] The technology's ability to create convincing fake images, videos, and audio has fundamentally challenged our ability to distinguish authentic from artificial content. Because of the wide availability of the tools to create "deepfakes" (synthetic media created using deep learning models), the malicious use of GANs does not require sophisticated actors. With limited audio, video, or even still images, a fake, yet convincing video can be created in minutes. These advances have blurred the lines between authentic and machine-generated content, making it almost impossible for humans to distinguish between such media.[8] The utility of such powerful technology has demonstrated far-reaching implications.

---

[6] See Gupta, P., Ding, B., Guan, C., & Ding, D. (2024). Generative AI: A systematic review using topic modelling techniques. *Data and Information Management*, *8*(2), 100066.

[7] See Shafik, W. (2025). Generative adversarial networks: Security, privacy, and ethical considerations. In N. R. Vajjhala, S. S. Roy, B. Taşcı, & M. E. Hoque Chowdhury (Eds.), Generative Artificial Intelligence (AI) Approaches for Industrial Applications (pp. 93–117). Springer Nature Switzerland; Bobby Chesney & Danielle Citron, Deep fakes: A looming challenge for privacy, democracy, and national security. 107 Calif. L. Rev. (Dec 2019), https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security.

[8] Ricker, J., Assenmacher, D., Holz, T., Fischer, A., & Quiring, E. (2024). AI-generated faces in the real world: A large-scale case study of Twitter profile images. *The 27th International Symposium on Research in Attacks, Intrusions and Defenses*, 513-30.

A recent prominent application involves deepfake technology for impersonation of Secretary of State Marco Rubio. By developing a convincing Signal handle, an unknown actor attempted to convince State Department officials that Secretary Rubio was seeking sensitive information.[9] Hany Farid, professor at UC Berkeley, explained that this type of impersonation is incredibly easy. "You just need 15 to 20 seconds of audio of the person, which is easy in Marco Rubio's case. You upload it to any number of services, click a button that says 'I have permission to use this person's voice,' and then you type what you want him to say," said Farid.[10] While impersonating a government official is a crime under 18 USC § 912, impersonating others is not necessarily a crime unless the conduct creates a financial impact.[11] Emotional, reputational, and physical harm resulting from a deepfake may not be criminalized, and based on the nature of the impersonation or publication of a deepfake, attributing the actor may be challenging and thus difficult to enforce.

More disturbing is the use of GANs to generate child sexual abuse material (CSAM). Unlike traditional CSAM, which requires the direct victimization of children, AI-generated material can be created without involving actual minors—yet it still fuels demand and normalizes exploitation. The Internet Watch Foundation identified over 20,000 AI-generated CSAM images in 2024, a 2,400% increase from the previous year.[12] The National Center for Missing & Exploited Children (NCMEC) reported that over the past two years, it has received more than 7,000 reports related to GAI-generated child exploitation. There are likely many more unreported or unidentified instances. As this technology becomes more pervasive and public awareness grows, we expect these numbers to grow.[13] Risks go beyond images. GAI manipulates children through realistic text prompts for grooming or exploitation. Offenders use GAI in sextortion, creating explicit AI images to coerce children into providing additional content or money.[14] Even AI-generated CSAM that does not ultimately resemble actual children can support the growth of the child exploitation market by normalizing child abuse.[15]

GANs also enable sophisticated disinformation campaigns. State and non-state actors use the technology to generate fake personas—complete with photos, social media histories, and biographical details—to spread false information and manipulate public opinion.[16] The Stanford Internet Observatory documented over 200 influence operations in 2024 that relied primarily on

---

[9] John Hudson & Hannah Natanson. (2025, July 8). A Marco Rubio impostor is using AI voice to call high-level officials. *Washington Post*. https://www.washingtonpost.com/national-security/2025/07/08/marco-rubio-ai-imposter-signal/.
[10] Id.
[11] See 18 U.S.C. Chap. 43 Part I.
[12] Internet Watch Foundation. *How AI is being abused to create child sexual abuse material (CSAM) online*. (2024 Update). Retrieved July 13, 2025, from https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/.
[13] NCMEC, The Growing Concerns of Generative AI and Child Sexual Exploitation, Dec. 13, 2024 (https://www.missingkids.org/blog/2024/the-growing-concerns-of-generative-ai-and-child-sexual-exploitation).
[14] See id.
[15] Campbell at 29.
[16] See Renée DiResta, *The Digital Maginot Line*, in INFORMATION WARS 45, 67-71 (2019).

GAN-generated content.[17] One recent disinformation attempt involved an AI-generated image of a fire at the Pentagon that spread rapidly on social media and was shared by RT, resulting in panic and even a dip in the stock market.[18]

C. Large Language Models: Automating Social Engineering

Large language models (LLMs), which can generate natural language for human-like text at scale, have revolutionized social engineering attacks by enabling criminals to conduct personalized, convincing conversations with victims.[19] These systems can adapt their approach based on victim responses, cultural context, and publicly available information to maximize success rates.

Typical malicious applications of LLMs involve automated phishing, elder fraud, and romance scams.[20] Bad actors deploy LLM-powered chatbots that engage potential victims in extended conversations, gradually building trust before requesting money or sensitive information.[21] LLMs also facilitate more sophisticated fraud schemes. LLMs can generate thousands of fake loan applications, each tailored to specific lender requirements and containing plausible but fabricated financial information. The AI system could produce applications faster than human reviewers could process them, overwhelming traditional fraud detection systems.[22]

---

[17] Josh A Goldstein, Jason Chao, Shelby Grossman, Alex Stamos, Michael Tomz, How persuasive is AI-generated propaganda?, *PNAS Nexus*, Volume 3, Issue 2, (Feb. 2024). The authors researched the question "Could foreign actors use AI to generate persuasive propaganda targeting audiences in the United States?" Using GPT-3, a now-comparably less advanced large language model, the researchers found the answer was a resounding and troubling yes, with minimal effort by the actor. Id.

[18] Shannon Bond, Fake viral images of an explosion at the Pentagon were probably created by AI, NPR (May 22, 2023).

[19] See Michelle Drolet, *10 Ways Cybercriminals can Abuse Large Language Models*, Forbes (June 30, 2023), https://www.forbes.com/councils/forbestechcouncil/2023/06/30/10-ways-cybercriminals-can-abuse-large-language-models/.

[20] Simon Moseley, Automating Deception: AI's Evolving Role in Romance Fraud, Centre for Emerging Technology and Security (April 2025), https://cetas.turing.ac.uk/sites/default/files/2025-04/cetas_briefing_paper_-_automating_deception_2.pdf. "AI's role in romance fraud extends far beyond text-based interactions. It is a force multiplier that enables large-scale, high-efficiency fraud and reduces the need for direct human effort." Id. at 20. See also FBI, Common Frauds and Scams, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams.

[21] See Moseley at 20-29.

[22] See Menish Gupta, Defending Against LLM-Based Financial Fraud: Best Practices and Recommendations, Hudson Data (Apr. 5, 2024), https://insights.hudsondata.com/defending-against-llm-based-financial-fraud-best-practices-and-recommendations/.

Criminal organizations increasingly use LLMs to generate malicious code and conduct cyberattacks.[23] The technology can automatically identify vulnerabilities in software systems and generate exploit code, democratizing advanced hacking techniques; because LLMs can generate malware, criminals without the necessary programming skill set to produce malware themselves can now hack into computer systems and exploit individuals.[24] Cybersecurity firms report exponential increases in cyberattacks in recent years—this increase is almost certainly the product of LLMs.[25]

II. Gaps in Current Criminal Law

While existing federal criminal statutes address many traditional crimes, significant gaps remain in addressing AI-enabled criminal activity. These gaps fall into three primary categories: jurisdictional challenges, evidentiary issues, and novel forms of harm.

A. Adequately Covered Criminal Activity

Several categories of AI-enabled crime fit comfortably within existing legal frameworks:

Financial Fraud: Traditional wire fraud statutes (18 U.S.C. § 1343) and mail fraud provisions (18 U.S.C. § 1341) generally cover AI-enabled financial crimes, regardless of the technology used. Courts have held that the use of sophisticated technology does not exempt conduct from fraud statutes.[26]

Identity Theft: The Identity Theft and Assumption Deterrence Act (18 U.S.C. § 1028) covers most AI-enabled identity theft, including the use of synthetic identities generated through machine learning.

Child Exploitation: Existing CSAM statutes (18 U.S.C. § 2252 et seq.) cover the distribution and possession of AI-generated child sexual abuse material, following the Supreme Court's reasoning in *Ashcroft v. Free Speech Coalition* that virtual child pornography lacking First Amendment protection can be criminalized. However, as discussed below, AI-generated CSAM presents challenges to legal enforcement and may be protected speech despite the potential harm.

---

[23] Mozes, M., He, X., Kleinberg, B., & Griffin, L. D. (2023). *Use of LLMs for illicit purposes: Threats, prevention measures, and vulnerabilities* (No. arXiv:2308.12833). arXiv.

[24] Id.

[25] "In 2017, the global damages inflicted by cybercrimes amounted to just over $1 trillion USD. However, by 2022, this figure ballooned to over $10 trillion USD, marking a tenfold increase in damages within a mere five-year span." Matthew Giannelis, Blog, AI-Powered Cyber Attacks – The Alarming 85% Global Surge, TechNews (Sept. 22, 2024), https://www.techbusinessnews.com.au/blog/ai-driven-cyber-attacks-the-alarming-surge/#.

[26] See *Van Buren v. U.S.*, 593 U.S. 374 (2021).

B. Critical Legal Gaps

Despite existing statutes that likely govern AI-assisted criminal offenses, significant gaps remain in addressing other AI-specific harms:

Deepfake-Specific Crimes: While some deepfake activities constitute fraud or harassment, no federal statute specifically addresses the creation and distribution of non-consensual deepfake imagery for purposes other than financial gain. The DEEPFAKES Accountability Act, introduced in the 116th Congress but never enacted, would have addressed this gap. CSAM produced using real children is constitutionally unprotected,[27] and AI-generated CSAM may be criminalized if it either depicts an actual, identifiable child or its training data set includes actual abuse imagery.[28] Otherwise, AI-generated CSAM images or videos are likely First Amendment-protected speech under existing Supreme Court precedent.[29]

AI-Generated Disinformation: Current law provides limited tools to address AI-generated disinformation campaigns, particularly those conducted by foreign actors. While the Foreign Agents Registration Act (22 U.S.C. § 611) requires disclosure of foreign influence activities, it predates AI technology. It contains significant enforcement challenges due to the difficulty in attributing AI-generated actions to specific foreign principals or agents, and the ambiguity regarding how autonomous AI systems fit within the legal definitions and requirements of FARA (i.e., are autonomous agents foreign actors?). These factors complicate identification, registration, and accountability of foreign agents operating via AI systems, potentially enabling covert foreign influence without clear oversight.

Algorithmic Bias Crimes: No federal statute addresses the intentional deployment of biased AI systems to discriminate against protected classes in criminal justice, lending, housing, or employment contexts. While civil rights laws provide some protection, criminal penalties for intentional algorithmic discrimination remain absent.

AI-Enabled Stalking and Harassment: Existing stalking statutes (18 U.S.C. § 2261A) may not adequately cover AI-powered harassment campaigns that use synthetic media or automated systems to target victims across multiple platforms.

Synthetic Media Authentication: No federal requirement exists for watermarking or disclosure of AI-generated content, making it difficult to distinguish authentic from synthetic media in criminal investigations. Given our criminal justice system's presumption of innocence until proven guilty beyond a reasonable doubt, the very existence of realistic AI-generated content can protect bad actors from accountability. Evidence for or against the defendant will require factfinders to determine its reliability and even legitimacy before rendering a guilty verdict. Seeing or hearing may no longer be sufficient for believing.

---

[27] Riana Pfefferkorn, Addressing Computer-Generated Child Sex Abuse Imagery: Legal Framework and Policy Implications, Lawfare (February 2024).
[28] Id.
[29] Id.

C. Emerging Threats Requiring Legislative Attention

Several emerging AI-enabled threats fall outside current criminal law:

AI-Powered Market Manipulation: Sophisticated AI systems can manipulate financial markets through coordinated trading strategies or the spread of synthetic information. While securities fraud statutes exist, they may not adequately address algorithmic manipulation techniques.

Autonomous Criminal Activity: As AI systems become more sophisticated, questions arise about criminal liability for autonomous systems that commit crimes without direct human control. Current law requires human intent, creating potential gaps as AI systems become more independent.

Cross-Border AI Crimes: Many AI-enabled crimes involve servers, victims, and perpetrators across multiple jurisdictions, creating complex questions about venue and jurisdiction that existing statutes do not clearly address.

III. Proactive Congressional Actions

Congress can take action to address AI-enabled crime through a comprehensive legislative framework that both regulates AI development and deployment and protects potential victims. This approach should include both preventive measures and enhanced enforcement capabilities.

A. AI Development and Deployment Regulations

Mandatory AI Impact Assessments: Congress could require companies developing AI systems with potential criminal applications to conduct and publish impact assessments evaluating the potential for misuse. Like environmental impact statements under the National Environmental Policy Act, these assessments would require developers to consider and mitigate criminal applications before deployment.

AI System Provenance Requirements: Congress could mandate that AI-generated content include embedded metadata or watermarks identifying its artificial origin. The DEEPFAKES Accountability Act's approach—requiring disclosure of synthetic media—should be expanded to cover all AI-generated content that could be used for criminal purposes.

Criminal Liability for Reckless AI Deployment: Congress could establish criminal penalties for companies that recklessly deploy AI systems, knowing they will likely be used for criminal purposes. This would parallel existing laws holding gun manufacturers liable for sales to prohibited persons while respecting legitimate AI development.

B. Victim Protection Measures

AI Crime Victim Compensation Fund: Congress could establish a compensation fund for victims of AI-enabled crimes, like the Crime Victims Fund established under the Victims of Crime Act.

Right to AI-Generated Content Removal: Congress should create a federal right for individuals to demand the removal of non-consensual AI-generated content depicting them, with civil and criminal penalties for non-compliance. This would address the unique harms caused by deepfake imagery and synthetic media.

Enhanced Identity Theft Protections: Congress should expand identity theft statutes to specifically address AI-generated synthetic identities and provide enhanced penalties for crimes involving AI-powered identity theft operations.

C. Law Enforcement Enhancement

AI Crime Task Forces: Congress could authorize funding for specialized AI crime task forces within the FBI and other federal agencies (including investigative agencies within the DoD, such as NCIS, CID, and AFOSI).

AI Forensics Capabilities: Congress should fund the development of AI forensics tools that can detect synthetic media, trace AI-generated content to its source, and analyze AI system behavior for criminal investigations.

International Cooperation Framework: Congress should authorize enhanced cooperation with international partners on AI crime investigations, including mutual legal assistance treaties specifically addressing AI-enabled transnational crimes.

Incentivize Research into Combating Harmful Use of AI: Congress should appropriate funds and authorize federal agencies to award grants and contracts for research into technologies, techniques, processes, etc., that identify, track, filter, or alert authorities or potential victims to AI-generated malware, media, or chats.

D. Constitutional Considerations

Any regulatory framework must carefully balance crime prevention with First Amendment and due process protections. The Supreme Court established that content-based restrictions on speech must survive strict scrutiny, even when applied to new technologies. Congress should focus regulations on criminal conduct rather than speech content, as restrictions must be narrowly tailored to compelling government interests. Specifically, a statute intended to criminalize the production, distribution, or possession with intent to distribute must be limited to criminalizing only prurient, patently offensive AI depictions of what appear to be minors that lack serious value, targeting obscene material rather than fictional youthful sexuality. Such a statute should connect culpability to harm-reduction rationale, including the inducement of real-world abuse, normalization of abuse, and undermining child protection efforts.

IV. International Approaches to AI-Enabled Crime

Approaches to AI regulation in international governmental organizations and nations are illustrative of how law and policy reflect unique values, principles, and ethics. Other countries

have adopted varying approaches to AI-enabled crime, providing both positive models and cautionary tales for U.S. policy development.

A. European Union: Comprehensive Regulatory Framework

The EU's AI Act, which entered into force in 2024, represents the world's most comprehensive approach to AI regulation.[30] The Act categorizes AI systems by risk level and imposes corresponding obligations, including:

- Prohibited AI Practices: The Act prohibits AI systems that employ subliminal techniques or exploit vulnerabilities to cause harm, directly addressing certain criminal applications.[31]
- High-Risk System Requirements: AI systems used in law enforcement must undergo conformity assessments and maintain detailed documentation.[32]
- Transparency Obligations: General-purpose AI models must disclose their capabilities and limitations, helping identify potential criminal applications.[33]

The EU has also established the European Centre for Algorithmic Transparency to monitor the compliance of AI systems and investigate potential violations.[34] This centralized approach contrasts with the U.S. system's reliance on multiple agencies and could inform Congressional consideration of a unified AI oversight body. Given our federal system, the EU offers relevant lessons learned to inform the development of compliance systems in the US.

However, the EU approach has faced criticism for potentially stifling innovation through over-regulation.[35] The Act's broad definitions and extensive compliance requirements may discourage AI development, although the debate centers around foreign companies (including U.S.-based corporations) arguing that the definitions and compliance regime set up confusion by introducing various rules in different markets, adding compliance costs and regulatory burden.[36] Nonetheless, recent announcements on the EU's Code of Practice for General Purpose AI have been met with approval from American companies that were initially outspoken critics of the AI Act.[37] Open AI

---

[30] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence, 2024 O.J. (L 1689) art. 43.
[31] Id. art. 5.
[32] Id. arts. 8-15.
[33] Id. art. 53.
[34] European Commission, *European Centre for Algorithmic Transparency*, https://algorithmic-transparency.ec.europa.eu/.
[35] European Commission, *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe* (2021) 104-5.
[36] See Luboslava Uram, *The EU AI Act: A Double-Edged Sword for Europe's AI Innovation Future*, Forbes (Jan. 23, 2025), https://www.forbes.com/councils/forbestechcouncil/2025/01/23/the-eu-ai-act-a-double-edged-sword-for-europes-ai-innovation-future/.
[37] See Open AI, *The EU Code of Practice and the Future of AI in Europe*, July 11, 2025, https://openai.com/global-affairs/eu-code-of-practice/.

credited its change of position to the EU's Code of Practice's simple and straightforward risk management regulations of models that balance transparency, responsibility, and safety with advancing businesses and the production of new technological advancements.[38]

B. United Kingdom: Sectoral Approach

The UK has adopted a more targeted approach, focusing on specific AI applications rather than comprehensive regulation.[39] Key elements include:

- Online Safety Act: Requires platforms to remove AI-generated harmful content and implement systems to detect synthetic media.[40]
- AI White Paper: Establishes principles for AI governance while allowing existing regulators to develop sector-specific approaches[41]
- Investigatory Powers Act: Provides law enforcement with enhanced capabilities to investigate AI-enabled crimes, including technical capability notices requiring companies to assist investigations.[42]

The UK's approach offers a middle ground between comprehensive regulation and innovation-minded policies, potentially providing a model for Congressional action that addresses criminal applications without stifling innovation.

C. China: State Control Model

China has implemented extensive AI regulations focused on state control and social stability rather than criminal law enforcement. Key measures include:

- Algorithmic Recommendation Management Provisions: Require companies to register AI algorithms with the government and prohibit recommendations that threaten national security.[43]
- Deep Synthesis Provisions: Mandate labeling of AI-generated content and prohibit synthetic media that spreads false information.[44]

---

[38] See id.
[39] UK Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation* (2023), https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.
[40] See Online Safety Act 2023, c. 50 (UK), https://www.legislation.gov.uk/ukpga/2023/50/.
[41] UK Department for Science, Innovation and Technology.
[42] Investigatory Powers Act 2016, c. 25, pt. 9 (UK).
[43] See Rogier Creemers et al., *Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022*, Digichina, Stanford Univ. (Jan. 2022), https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/.
[44] Zhang, Laney, *China: Provisions on Deep Synthesis Technology Enter into Effect* (2023), https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/.

- Draft AI Measures: Propose comprehensive licensing requirements for AI development and deployment.[45]

While China's approach demonstrates the feasibility of extensive AI regulation, its focus on state control rather than individual rights makes it unsuitable as a model for U.S. policy. However, China's technical requirements for content labeling and algorithm registration could inform more narrowly tailored U.S. approaches.

D. Singapore: Innovation-Friendly Framework

Singapore has developed an AI governance framework that balances innovation promotion with risk management.[46] Key features include:

- Model AI Governance Framework: Provides voluntary guidance for AI development and deployment, focusing on risk management rather than mandatory compliance.[47]
- AI Verify Foundation: Establishes technical standards for AI testing and validation, helping identify potential criminal applications.[48]

Singapore's voluntary approach has encouraged industry adoption while maintaining flexibility for emerging technologies. This model could inform Congressional consideration of incentive-based rather than mandate-based approaches to AI crime prevention.

E. Comparative Analysis and Lessons for Congress

These international approaches offer several lessons for U.S. policy:

Regulatory Clarity: The EU's detailed requirements provide certainty for industry but may discourage innovation. Congress should focus on clear, narrow prohibitions focused on the malicious or harmful use of an AI model rather than broad regulatory frameworks that prevent the research and development of a technology.

Sectoral Flexibility: The UK's approach of allowing existing regulators to develop AI-specific rules within their domains could work well within the U.S. federal system, where agencies like the FTC, SEC, FCC, and NIST already have relevant expertise.

Technical Standards: Singapore's focus on technical standards for AI validation could help law enforcement agencies develop forensic capabilities while supporting industry self-regulation.

---

[45] Zhang, Laney, *China: Generative AI Measures Finalized* (2023), https://www.loc.gov/item/global-legal-monitor/2023-07-18/china-generative-ai-measures-finalized/.

[46] Personal Data Protection Commission, *Singapore's Approach to AI Governance*, https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework.

[47] Id.

[48] AI Verify Foundation, *AI Verify Testing Framework*, https://aiverifyfoundation.sg/what-is-ai-verify/.

International Cooperation: All major jurisdictions recognize the need for international cooperation on AI-enabled transnational crimes. AI facilitates the perpetration, scaling, and evasion of transnational crime. Congress should prioritize mutual legal assistance frameworks and information sharing agreements.

V. Recommendations

The criminal exploitation of artificial intelligence represents an unprecedented challenge requiring immediate Congressional action. The technologies discussed—computer vision, GAI, and LLMs—are already being weaponized by criminal actors, and the pace of AI development ensures that new threats will emerge faster than traditional legislative processes can address them.

Congress should adopt a three-pronged approach to combat the use of AI to enable criminal and abusive acts:

1. *Target criminal law reforms addressing specific AI-enabled harms*, such as including sentencing aggravators for existing crimes (i.e., stalking, extortion, etc.) for defendants who used AI to facilitate the commission of the offense. Criminalizing the use of data or files to create digital models that facilitate the creation of AI-generated CSAM and taking steps to encourage other nations to do the same will help protect our most vulnerable citizens. Currently, the application of existing law appears insufficient to deter malicious use of AI, and the content of existing law does not criminalize AI-enabled acts that can cause significant harm.

2. *Support state, local, or federal regulations that prevent harm and promote safety*, such as requiring AI developers to consider and mitigate criminal applications, including requirements for models used for consequential actions, to obtain independent, third-party safety and risk reviews.

3. *Enhance law enforcement capabilities* for investigating and prosecuting AI crimes, including increased budgets to acquire AI capabilities and appropriate training to counter AI-enabled offenses. Given the limited resources available to law enforcement, states can create a private cause of action for individuals or classes harmed by an actor's malicious use of an AI system by a third party or the unintended, but reasonably foreseeable consequence of an AI system's behavior, against the actor or, in the latter case, the model's developer.[49]

With each of these lines of effort, there are technical, policy, and legal obstacles that should be considered. Given the rapid pace of technological advancement in AI-enabled capabilities and the limitless imagination of bad actors in leveraging these advancements, Congress should

[49] See Consumer Reports, Consumer Protection Policies for the AI Era (https://innovation.consumerreports.org/cr-publishes-artificial-intelligence-policy-recommendations/)

consider technology-agnostic approaches to deter and punish harm caused using AI that is not already covered by Title 18, United States Code. Such harms include defamation, biased or discriminatory decisions, economic damage, emotional and psychological harm, mass surveillance, and misinformation at scale. These categories of harms are typically not criminalized, for good reason. Misinformation, for example, is likely protected under the First Amendment. However, the potential harm of misinformation at scale is comparable to other legal exceptions to constitutionally protected speech, like incitement or true threats.

Effective AI crime prevention requires striking a balance between promoting innovation and ensuring public safety. The EU's comprehensive approach may discourage beneficial AI development, while permitting a market-driven, purely voluntary framework to develop will likely prove insufficient to address sophisticated criminals.

Areas that Congress should consider for further action include:

- Instituting specific criminal penalties for non-consensual deepfake creation and distribution
- Supporting federal regulations and standards that require AI-generated content labeling and authentication to help distinguish real and generated content
- Enacting enhanced penalties for crimes involving AI tools when the use of such tools aggravates the crime
- Increasing funding for law enforcement's AI forensics capabilities
- Developing international cooperation frameworks or ratifying treaties aimed at preventing and prosecuting transnational AI-enabled crimes
- Increasing dialogue and discourse about AI across states' attorney generals and legislatures to increase awareness of risks, trust in law enforcement, and sharing of best practices in preventing and combating AI-enabled crime
- Seeking perspectives from industry, research organizations, federal agencies, and private citizens on balancing risks of regulating AI and other public policies, such as protecting innovation, freedom, and security

Conclusion

When determining the appropriate legal structures in the U.S. affecting AI development and deployment, it is crucial to recognize a fundamental truth about AI: it is a ubiquitous technology enabler that can be leveraged to assist in accomplishing various tasks that typically would require human intelligence. By focusing on regulating the use and impact of a model that could, or does cause harm, rather than the research and development of a model that could be used for societal good, Congress can strike the appropriate balance of protecting society while preserving freedom; upholding justice while protecting privacy; enabling progress while preventing chaos. For all the new risks that AI presents to our society, it also can ignite revolutionary economic growth, scientific discoveries, and ensure our security and prosperity.

With understanding, skill, and data, AI systems can help humans accomplish many tasks more effectively and efficiently. Still, AI does not discriminate, regulate, or prevent harm if bad actors choose to deploy those systems maliciously. The more authority we delegate to AI systems, the

more likely such systems will create harm inconsistent with the human deployer's intent, giving rise to the need to develop systems of accountability, possibly through criminal liability, for upstream actors as well. Some bad actors already use AI to carry out crimes, and some use AI to harm individuals and society in ways that are not currently illegal. It is a safe prediction that more bad actors will use AI and more harm will be caused by that use. The window for proactive action is rapidly closing. Sophisticated AI systems enable powerful capabilities. These systems are rapidly proliferating, and bad actors can exploit these capabilities easily and relatively cheaply. Meanwhile, law enforcement risks falling further behind without funding or legal structures to support their mission to serve and protect our communities and our most vulnerable citizens. The United States can choose to shape the intersection of AI and criminal law proactively, or it can reactively respond to an escalating series of AI-enabled crimes that will likely outpace our legal and enforcement capabilities.

Thank you for your attention to this critical issue. Robust discussion and debate on this issue, consistent with our national values, are necessary to combat AI-enabled harms meaningfully, now and in the future. I look forward to your questions and to working with this Subcommittee on comprehensive solutions that protect Americans while preserving the innovation that drives our technological leadership.

Mr. BIGGS. Thank you, Dr. Bowne, and we have your written testimony, which is more expansive, so I remind everybody we have that, so appreciate that.

Ms. Perumal, we give you your five minutes now.

STATEMENT OF ZARA PERUMAL

Ms. PERUMAL. Chair Biggs, Ranking Member McBath, and the Members of the Committee, thank you so much for the opportunity to testify today and for creating this forum to discuss how AI is changing the landscape of cybercrime. I am honored to share my perspective on how technology is making these threats more accessible, more personalized, and more difficult to detect.

My name is Zara Perumal. I am the Co-Founder and CTO of OverWatch Data, a cyber threat intelligence company that use AI to identify and analyze emerging threats in the cybercrime and fraud ecosystems. Through our work, we see every day how AI is used to both prevent and also to facilitate criminal activity.

I would like to focus my remarks today on how we see AI changing the threat landscape and what we can do about it through both education and innovation. AI is a powerful, general-purpose tool with a broad range of applications for criminal activity and for a broad range of threat actors. It can be used to learn how to commit crimes, to write code and craft realistic scam text messages, generate audio or voice clones, and of course, create deepfake images or videos.

Across this wide range of malicious use, three trends stand out.

First, AI is reducing the barriers to entry for cybercrimes. Users can ask a chatbot including ones explicitly designed for fraud how to commit crimes. They can learn the technical skills they need to carry them out and they can also use it to make their attacks more convincing and more effective.

Second, it is challenging businesses by subverting identity verification systems. AI can be used to generate a photo for a fake persona or profile. It can then be used to generate high quality synthetic fake IDs and then if they are asked to verify their identity, they can join a video called swap bare face with their fake photo and verify their access to that business. This is a problem not just for the specific business that is being targeted, but it is a problem because it gives them a foothold from which they can hide their identity for the future next online crime that they will carry out.

Third, we see is the crimes that are becoming far more personalized. For example, voice clones are used to target the elderly by calling a grandparent and what sounds like their grandchild's voice and claiming to be in the hospital and in need and in need of money. Employment scams prey on young adults who are looking for their first job. One of the most disturbing cases is the nudifying apps which often target children. They turn ordinary photos into fake sexually explicit images which are then used to bully, harass, and extort victims, in some cases driving them to suicide. This abuse is carried out to children, both by their classmates and by remote criminals.

There is a lot of harm. There is a lot that is changing, but there is also a lot we can do.

First, education awareness can prevent and deter many of these harms. These crimes work because people don't expect them. If we invest in education across schools, workplaces, and communities, we can make these crimes less effective and more costly to carry out.

Second, we have an opportunity to combat this with innovation. The same technology that is enabling these crimes, can also be used to detect scams, find malware, and destruct cybercrimes. By supporting innovation and strengthening public/private partnerships, we can shift the technical advantage to the defenders.

While AI enables crime to be more accessible, more personalized, and harder to detect, I remain optimistic. With the right investment in education and innovation, we can engage our whole society in building a future where AI expands access to opportunities, strengthens safety, and helps people spend more time on what matters.

On a personal note, it is very exciting to me to see that Congress is addressing this issue and putting a spotlight on it. Thank you and I look forward to your questions.

[The prepared statement of Ms. Perumal follows:]

"Artificial Intelligence and Criminal Exploitation: A New Era of Risk"

July 16, 2025

Hearing Before The
Subcommittee on Crime and Federal Government Surveillance
Of the Committee on the Judiciary

Prepared Statement by
Zara Perumal
CTO/Co-Founder
Overwatch Data

Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee, thank you for the opportunity to testify today, and for creating a forum to examine how artificial intelligence (AI) is changing the landscape of cybercrime. I am honored to share my perspective on how this technology is making these threats more accessible, more personalized, and more difficult to detect.

I am the Co-Founder and Chief Technology Officer (CTO) of Overwatch Data, a cyber threat intelligence company that uses AI to identify and analyze emerging threats in the cybercrime and fraud ecosystems. Through our work, we see every day how AI is used both to prevent and to facilitate criminal activity.

AI is a powerful general-purpose tool that allows users to enhance skills, learn, and create innovative solutions for complex problems with greater efficiency. However, the same capabilities can be exploited by bad actors to learn how to commit crimes, develop new methods of fraud or theft, and generate scam or sextortion content. This can cause significant harm, including major financial loss and, in extreme cases, emotional distress leading to suicide.

Overwatch Data's analysis focuses on where AI is most significantly changing the threat landscape. Specifically, what are the new threats, what are the most likely threats, and what are the most harmful threats?

What This Means: Impacts on Users, Businesses, and the Criminal Ecosystem

One of the most immediate changes is how generative AI lowers the barrier to learning, executing, and scaling cybercrime and fraud. Tasks that once required technical expertise, such as writing convincing scam messages or creating phishing pages, can now be completed using AI tools. The outcome is a flood of spam texts, emails, phone calls, and social media messages that

occur more and more often[1]. These messages are personalized, translated, and delivered at scale, making scams more convincing, more widespread, and more accessible to individuals with little or no technical background or understanding of how to commit crimes.

More novel uses of AI combine voice, image, and video understanding for more personal attacks. Scammers use voice clones built from social media posts to impersonate a loved one in distress. Victims receive urgent calls from what sounds like their family member, claiming to be injured. Some are also sent fake hospital photos to make the lie more convincing. These scams target our instinctive human trust in hearing a loved one's voice, and our willingness to do anything to help them.

Even more disturbing, nudifying apps use AI to digitally remove clothing from non-explicit photos, generating fake sexually explicit images. Threat actors use these tools to transform ordinary photos into explicit content and then weaponize the results to seek revenge, extort money, or manipulate their victims. Although the images are fake, the shame and fear they create are real. In some cases, victims have comited suicide as a result. This abuse has affected people of all ages, including children who have been targeted by their classmates, online predators, and coordinated bot networks.

In addition to personal harms, these tactics impact small and large businesses. A growing trend is using AI to subvert identity verification systems, including "Know Your Customer" checks, by generating fake photos, high-quality synthetic IDs, and even live deepfakes to pass as legitimate users. This allows criminals to access and exploit online services with reduced risk of detection. In addition, more effective social engineering through text messages and video, such as impersonating executives on live video calls, creates new risks and financial losses ranging from fraud to malware deployment.

This ecosystem evolves rapidly. The models and techniques that were state-of-the-art last year are now out-of-date and replaced with newer models. As the tools evolve, one thing remains consistent: attackers exploit our trust in one another and our outdated understanding of cybercrime. Many people still picture clumsy, typo-filled phishing emails, not the highly personalized and realistic scams that are common today.

To combat this, we cannot keep operating in the status quo. We need a whole-of-society approach, starting with education and awareness for children, extending to communities, businesses, and nonprofit organizations. It also requires a coordinated push to encourage innovation, improve information sharing, and strengthen response efforts across tech companies, telecom providers, financial institutions, and law enforcement. Each organization has different pieces of the puzzle, and unique enforcement capabilities to deter crime. No single organization can tackle this problem alone.

[1] https://www.cnet.com/tech/services-and-software/scams-survey-2025/

Adjacent Trends, Complicating Factors, and the Future of AI use for Crime

As we look at the threats that are already here, we also consider emerging trends in AI and cybercrime that offer insight into where this space may be headed.

1. **Agentic AI:** Agentic AI is the next trend in AI that is already here. Instead of just static models that generate outputs solely based on training data and prompts, agents use tools, query data, and interact with each other. This enables AI agents to be more proactive and learn by doing. As a result smaller, less sophisticated and cheaper models can have an outsized impact when deployed as part of an agent, especially for narrow or high-impact use cases. This ability to adapt through trial and error makes agents more convincing and capable, especially in tasks that involve persuasion, like crafting text messages or mimicking human behavior.

   A particularly new development is computer-use agents. These are AI systems that can operate a computer much like a human user. Using computer vision, they can see the screen, click buttons, and navigate software tools. This gives them access to a wide range of capabilities that were previously out of reach.

   Because they can take real actions, these agents are uniquely qualified to be effective in fraud. Unlike traditional bots that follow fixed scripts, computer-use agents can adapt to feedback and navigate interfaces like a human. Given a high-level description of a scam, they may be able to figure out the steps, adjust as needed, and complete the task in ways that are harder to detect and more persistent than past systems.

2. **World Models:** This is an area where AI experts think the state of the art for AI will move. Unlike models trained solely on text, images, or internet content, world models aim to simulate the physical world[2] and understand cause and effect. Mimicking how we learn about gravity and the physical world in school, these models incorporate a common-sense understanding of the world.[3] This approach may lead to a much more nuanced understanding of the physical environment.

   If AI grows in this direction, it could lead to more advanced impersonation, such as deepfake videos with realistic, live-looking backgrounds. World models may also enable more real-world crime, such as improving reconnaissance and information gathering of physical environments, by allowing AI systems to understand physics and navigate physical spaces.

3. **Growth of Individual User Data Footprint:** The more online data an individual has, the more vulnerable they are to cybercrime. Many people conduct much of their lives online through social media, online banking, medical apps, and commuting tools. Personal information is stored in public and private records and often ends up in leaked databases after service breaches. This includes phone numbers, emails, passwords, addresses, and

[2] https://www.linkedin.com/posts/yann-lecun_lots-of-confusion-about-what-a-world-model-activity-7165738293223931904-vdgR/

[3] https://ai.meta.com/blog/v-jepa-2-world-model-benchmarks/

family connections. Video, photos, and audio content are widely shared on social media, making it easier to clone identities. Such data fuels social engineering, enables AI misuse, and increases the surface for attacks. The more available, and the less secure personal data is, the more vulnerable we are to AI enabled cybercrime.

With this in mind, we expect AI-enabled crime to continue to be more tailored, adaptive, and pervasive. In light of that, we need to be clear about the future we are working towards.

The Future We Want: How to Evaluate Success in Combating AI-Enabled Crime

I, along with the whole team at Overwatch Data, work every day to contribute to a future where AI helps solve real problems, expands access to resources, and creates new opportunities. A future where people spend more time on what matters, and where built-in defenses make harm harder to carry out.

We often talk about regulation in terms of slowing down the bad outcomes. That matters. We want to deter abuse and make crime more expensive and difficult. But we should also see regulation as a tool to accelerate progress toward positive outcomes. It can guide innovation in the direction we want to go. It is just as important to focus on the future we want to build as it is to prevent the harms we want to avoid.

For many *existing* models and capabilities, we cannot put the genie back in the bottle. The models that enable the harms we've discussed have been shared, reshared, cloned, and compressed or distilled into smaller, more efficient versions. These “minified” models can replicate similar capabilities with fewer resources, making them easier to distribute and use. As we work to mitigate the harms of current models and limit the risks from future ones, we should focus on the end goal.

If it is inevitable that these models will eventually be accessible, what does a good end state look like?

This end state should ultimately guide how we measure success. Addressing AI-enabled crime is complex and every option, including doing nothing, comes with tradeoffs. As we consider what actions to take, we should first ask: How would we evaluate the outcomes? What would success look like in practice?

To ground that vision in practice, here are some of the questions that should be continually asked as both government and industry shape responses to AI-enabled crime:

1. **Compliance: What is the cost (time/money) for legitimate users?** Good faith businesses and individuals must be able to practically comply, so it matters if it is as easy as filling out a quick form, or a laborious process differing across jurisdictions. Groups of people/businesses will have differing financial means and abilities to comply.
2. **Intent OR Use: Who has to act in good faith for this to work?** If we ban certain models, or use cases, cybercriminals are unlikely to comply. The systems we put in place must be effective when those who act in good faith comply, but the bad actors do not.

3. **Risk Analysis: How does this compare the alternative?** When we ban an activity or make it difficult, threat actors often adapt to using the next easiest option. For example, if they cannot use deepfake imagery, threat actors may go back to pulling imagery off of social media or using stock photos. It is important to know what that option is and the impact to their operations by shifting them to their backup option. We should identify where those alternatives impose significantly higher costs in time, money, or risk to the criminal ecosystem.
4. **Adaptability: How does this intervention adapt?** Because AI models and illicit use cases are evolving so quickly, any actions or policy we make needs to evolve quickly.
5. **Interdependencies: What other areas of innovation does this affect?** Because AI is often multi-purpose, any change aimed at reducing cybercrime may also affect other innovations that benefit society, including those working to combat cybercrime itself.

Specific Recommendations

1. Empower Societal Resilience

Strengthen AI and Cybercrime Literacy Across Society

AI-enabled crime exploits the fact that we do not expect it. The level of personalization catches people off guard and reaches them when they are most vulnerable. From voice clones to romance scams to sextortion, these scams often target vulnerable groups like children and the elderly. Children are among the most active users of technology and have been both victims and perpetrators[4] of AI-enabled abuse. We need to engage them directly in the solution and give them the tools to prevent harm.

If we push education about cybercrime and AI across schools, businesses, and community organizations, we deter AI-enabled crime by making it less likely to work. As we grow awareness of how AI can be used for both harm and good, we make our society less vulnerable to abuse and better positioned to take advantage of its benefits.

Efforts like the Redirect Project, which teaches elementary students about cybersecurity and online harms, and Operation Shamrock, which shares scam tactics with communities, show how awareness efforts may take shape. Tools like Birdwatch and scam reporting platforms let people flag threats and share alerts in real time.

We should prioritize and fund education especially for vulnerable populations to deter crime.

2. Shift the Technical Advantage to the Defenders

Leverage AI for Defense

The same tools used to commit cybercrime can be used to stop it. If threat actors use AI to scale scams, we can and should use it to detect and block them. If they build malware that adapts, we can build systems that learn to defend. As agents are used to find and exploit vulnerabilities[5], we

[4] https://www.redirectproject.org/
[5] https://www.helpnetsecurity.com/2025/06/25/xbow-ai-funding/

can use those same approaches to automatically find active vulnerabilities in systems and patch them before code is deployed. If they create “fraud-as-a-service tools”, we can use AI to trace, disrupt, and dismantle those operations. AI can also help us stay ahead of threats by surfacing emerging tactics, spotting trends, scoring the risk of attack methods or vulnerabilities, and identifying patterns before they scale. This is how we move from human speed to digital speed in fighting cybercrime. Scaled offense necessitates scaled defense.

We should use AI to prevent and disrupt crime; however, it does not have to be everywhere all at once. We can be deliberate about where, when, and how we use it. We should use it to leverage its opportunity while mitigating risks like hallucination and model inaccuracy.

For example, using AI with humans in the loop to make decisions enables AI to improve the efficiency review process while the human makes the final decision. Additionally, AI can be built with transparency in mind: having systems that cite their sources, or show their reasoning, makes it easier for humans to review, question and audit the outputs. By building this way, we can leverage the speed and scale at which AI can understand data with the trustworthiness of human-expert review.

By finding ways to support AI-driven cybersecurity innovation and enabling public-private collaboration, Congress can take a massive step in ensuring defenders are not outpaced by attackers.

Institutionalize Red Teaming and Bug Bounty Programs for AI Tools

High-risk and general-purpose AI systems should undergo structured adversarial testing to identify misuse pathways before they cause harm. Like red teaming in cybersecurity, this helps uncover risky edge cases and misuse scenarios that standard evaluations may miss. Alongside this, funding bug bounty programs to reward responsible disclosure of jailbreaks, synthetic identity generation, and other forms of AI abuse. Running adversarial testing across a range of harmful use cases (e.g. physical crimes, malware, fraud, extortion) helps make it harder to use. Notably AI can help develop red teaming systems, and make it cheaper and easier to implement.

3. Align Institutions and Infrastructure Across Society

Support Public-Private Disruption of AI-Enabled Crime

Investing in infrastructure and legal tools can enable joint action between industry and government to disrupt platforms that support AI-driven fraud, scam distribution, or impersonation services. Examples like Information Sharing and Analysis Centers (ISACs) and the National Cyber-Forensics and Training Alliance (NCFTA) show how coordinated information sharing and disruption can work in practice. Efforts like the Internet Crime Complaint Center are also incredibly helpful in engaging a collective response based on real world harm. Reducing barriers to cooperation can make these partnerships faster, broader, and more effective.

Frame AI Policy Around Concrete Harms

Regulation should focus on clear, observable harms like impersonation scams, nudification abuse, and synthetic ID fraud. A harm-based approach allows policy to stay flexible as AI evolves, while staying aligned with how law enforcement investigates and responds to abuse.

Promote Shared Responsibility for Dual-Use Technologies

Addressing AI-enabled crime is a whole-of-society challenge. Companies building general-purpose AI tools, along with other infrastructure providers, should share responsibility for reducing foreseeable misuse. This includes safeguards such as access controls, usage monitoring, and clear reporting channels. For high-impact systems deployed at scale, small investments in prevention can significantly reduce downstream harm. As with other technologies that shape communication and access broadly, coordinated responsibility is essential to reducing misuse.

AI-enabled crime is evolving quickly. It is making threats more accessible, more personalized, and more difficult to detect. These are not one-size-fits-all problems. We are dealing with complex, general-purpose technologies that can be used to help or to harm. That complexity demands solutions that are just as comprehensive, tailored, and adaptive. I am optimistic that we can meet this challenge. With the right investment in education, innovation, public-private partnerships, and a whole-of-society approach, we can mitigate harm while enabling innovation. We can build a future where AI expands access to opportunity, strengthens safety, and helps people spend more time on what matters.

Thank you, and I look forward to your questions.

Addendum 1: Criminal Use by AI Capabilities

AI tools are being used to enable a wide range of criminal activity. The following examples outline key capabilities and the harms they enable.

1. Language and Cultural Fluency

Capability:

Large language models (LLMs) can generate fluent, grammatically correct, and culturally specific messages in dozens of languages. These models mirror the tone, structure, and formatting of government notices, company messages, or support requests. Jailbroken and open-source versions allow this capability to be used without guardrails that prevent malicious use[6].

Harm 1: Phishing for Login Information

For years, in cyber security training we taught people to look for obvious typos or grammatical errors in emails, but with AI the obvious indicators are disappearing . Criminals use AI to create phishing emails and scam texts that closely resemble legitimate messages. In one 2024 case, French drivers received toll payment scams written in fluent, region-specific French. The messages linked to a cloned toll agency website that looked official and used accurate branding[7] [8]. Similar toll/traffic scams are trending across the US[9]. These scams can be delivered as text messages, business emails or through other messaging platforms.

Harm 2: Job/Recruitment Scams

AI has also been used to enhance employment scams. Threat actors use LLMs to generate professional-looking job descriptions, interview instructions, and recruiter messages. These scams may aim to collect personal information such as Social Security numbers or bank details, or trick jobseekers into sending upfront payments for fake roles. The improved fluency and formatting make these messages more convincing and more difficult to detect, especially for younger or international applicants.[10,11].

[6] https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf
[7] https://natlawreview.com/article/growing-cyber-risks-ai-and-how-organizations-can-fight-back
[8] https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf
[9] https://www.fox13news.com/news/scammers-using-ai-improve-toll-text-message-scam-targeting-drivers-constantly-getting-smarter
[10] https://www.anthropic.com/news/detecting-and-countering-malicious-uses-of-claude-march-2025
[11] https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf

Harm 3: Investment and Cryptocurrency Scams

Scammers use LLMs to craft persuasive language for fraudulent investment opportunities, including fake cryptocurrency platforms[12], trading schemes, and tech startups[13]. These scams are often distributed through social media and messaging apps or sent directly via text. AI-generated content allows scammers to mimic professional investment language, write promotional materials, and respond convincingly in real time. These scams frequently target younger adults or gig workers seeking financial growth or remote income opportunities.

Harm 4: Romance and Emotional Scams

Language models are increasingly used to automate romance scams and emotionally manipulative fraud. These scams involve building trust over time through AI-generated conversations on dating sites or messaging apps. With minimal effort, one scammer can manage dozens of victims using emotionally tailored messages.

Once a relationship is established, the conversation often shifts to urgent financial requests or fraudulent crypto investments. AI is used to maintain tone, personalize messages, and generate real-time responses in multiple languages.

Investigations have confirmed the use of LLMs in long-form romance scams and crypto fraud, with chatbots managing victim grooming and scripted emotional appeals. These scams are devastating to victims causing both incredible financial losses[14] and in some cases leading victims to suicide[15].

Romance scams can be conducted by a range of threat actors, including scam compounds that rely on coerced or trafficked labor[16].

2. Synthetic Image and Video Generation

Capability:

AI tools can generate or alter human images in ways that look realistic. This includes creating synthetic faces to generate people, editing images or videos through faceswapping, or voice-syncing and removing clothing from existing photos using nudification models. Nudification tools may either digitally undress a photo or take a nude image and faceswap the victims face onto the source image. These tools are available through a variety of platforms,

[12] https://xss.as/threads/140320/post-994654/31e9671f625e0f1021272eccf5aa3543

[13] https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf

[14] https://www.dailynews.com/2024/10/13/how-pig-butchering-romance-scams-siphon-millions-from-californians-every-year/

[15] https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk

[16] https://www.amnestyusa.org/press-releases/cambodia-government-allows-slavery-and-torture-to-flourish-inside-hellish-scamming-compounds/

ranging from open-source models that require technical expertise to user-friendly options like Telegram bots. These bots let users upload a photo and receive a manipulated image such as a nudified or face swapped version directly in the chat, without needing to write code or install software.

Harm 1: Generating Synthetic Faces for Fake Identities

Threat actors use AI generated photos for a variety of purposes. A common use is for ID fraud or "Know Your Customer" (KYC) bypass[17]. In this use case, threat actors create fake images to go with a fake ID and use it to register for a fake account that they may use for other crimes. Criminals pair these images with fake backstories and documents to pass onboarding checks[18]. Since new images are generated on demand, it is harder for platforms to flag or verify these images using traditional detection systems.

Harm 2: Nudification of Images

AI generated nude photos are often used for revenge, sextortion or harassment. Even though they are fake, they can be used for extortion by the sense of shame that would be felt if it were released in some case driving the victims to suicide[19]. In some cases this is cyberbullying from other students[20], in other cases it is remote and coordinated cyber crime gangs[21]. This is prevalent[22], Wired notes Telegram bots list more than 4 million monthly users for undressing photos[23].

Harm 3: Romance Scams

Image and video content add realism for romance scams[24]. Romance scams may be done by both individuals or organized crime networks.[25] AI tools for deepfake are directly listed for use for romance scams.

---

[17] https://darkforums.st/Thread-BYPASS-KYC-VERIFICATION-USING-DEEPFAKE-GUIDE?pid=86841#pid86841/6eece5704354d66c69bafc5e31f9fe73

[18] https://www.overwatchdata.ai/blog/the-dark-side-of-ai-fraudsters-new-arsenal

[19] https://www.wsj.com/tech/personal-tech/sextortion-scam-teens-apple-imessage-app-159e82a8?st=TWuAaq&reflink=desktopwebshare_permalink

[20] https://6abc.com/francesca-dorota-mani-ai-generated-pornographic-images-westfield-high-school-nj-legislation/14019614/

[21] https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

[22] https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

[23] https://www.wired.com/story/ai-deepfake-nudify-bots-telegram/

[24] https://frankonfraud.com/haotian-ai-providing-deepfake-ai-for-scam-bosses/

[25] https://www.wired.com/story/pig-butchering-scam-invasion/

Harm 4: Executive or Business Impersonation

Deepfake videos have also been used to impersonate business executives. Whether used to directly authorize the transfer of money (millions of dollars in some cases[26]) or as a lure to gain initial access to an organization[27] executive deepfakes can be effective since people have a general sense of their likeness but may not know them directly, they have trust and authority, and if a senior executive sends an employee something people are less likely to ask questions.

Harm 5: Scam Enablement

Other scams use celebrity deepfake imagery to lend credibility to fake or low quality products[28]. Using the likeness of a celebrity to support a new cryptocurrency, supplement, or product then sharing it on social media can help people buy it quickly, exploiting their trust in that celebrity's brand.

3. Voice and Face Cloning for Impersonation

Capability:

AI tools can clone a person's voice or simulate their face using only a few seconds of audio or video. The easiest clones operate from a few images or short audio clips using accessible online tools. These may be convincing at a glance or for short recordings. For more skilled actors who fine-tune models or run tools locally, more realistic clones can be produced with relatively little source material.

With more content, such as an hour and a half threat actors can generate "studio quality" voice clones from online tools that are realistic to friends of family. When we think about the availability of content on social media, let alone for public figures, making clones is incredibly achievable.

Voice cloning replicates tone, cadence, and emotional delivery with high accuracy. Face cloning tools generate realistic video by syncing a person's facial expressions and speech, often in real time. In combination with tools like DeepFaceLive and OBS Studio, threat actors can produce and stream live video content via transformation in addition to static content.

Harm 1: Family Emergency Scams Using Cloned Voices

Scammers use AI to impersonate relatives in distress, often targeting elderly victims. In one 2025 case on Long Island, fraudsters cloned the voice of a grandchild using audio from TikTok and voicemail greetings[29]. The victims of this fraud ring receive calls pretending to be their

[26] https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea
[27] https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis
[28] https://www.rollingstone.com/tv-movies/tv-movie-news/tom-hanks-warns-ai-deepfake-scam-likeness-1235092071
[29] https://nypost.com/2025/05/23/us-news/long-island-officials-warn-new-scam-uses-tiktok-and-ai-simulated-voices-to-impersonate-grandkids-and-rip-off-seniors

grandchild in jail, or in the hospital, in need of an urgent money transfer. The combination of hearing a loved one's voice, and our willingness to do anything for those we love makes this scam particularly effective. In some cases this is paired with imagery such as deepfake images of their child in a hospital bed.

Harm 2: Executive Impersonation in Financial Fraud

AI-generated face and voice clones have been used to impersonate corporate leaders in live video calls. In one case in 2025, attackers used a deepfake of a CFO[30] to instruct staff to process a $25 million transfer. The clone was realistic enough to convince the employee on the call, and again exploit our trust in what we see with our own eyes.

Harm 3: Bypassing Voice Authentication and Account Security

Voice cloning has also been used to attempt bypassing voice-based authentication systems used by banks and customer service centers. A cloned voice can be used to impersonate a customer, reset credentials, or approve financial actions over the phone. These attacks challenge the reliability of biometric security tools[31].

4. Code Generation and Exploitation

Capability:

AI models can generate and understand code. This can be used to generate malware more effectively, disguise who wrote it, and make variants so it is harder to detect. In many cases this is possible with mainstream hosted models since the line between good and bad use cases is not always obvious. In other cases, attackers use jailbreaks, which are prompting techniques that bypass safety filters, or fine-tuned open-source models that have been retrained on malicious content to enable more obviously harmful use cases[32]. On darkweb forums, users share both models finetuned for malware generations, and jailbreaks or tools to use open source models for malware generation[33], and guides to build your own “hacker assistants”.

Harm 1:Malware and Credential Theft

Threat actors have used AI tools to develop malware, both for those with minimal coding experience and for those with more advanced understanding of software systems. AI assists with development across multiple languages, helps attackers learn coding practices, and speeds up their overall workflow. Especially in malware use cases, threat actors may use multiple or stolen accounts to hide their activities across chat sessions to evade detection.

[30] https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea
[31] https://ici.radio-canada.ca/nouvelle/2143502/reconnaissance-vocale-ia-banques-securite
[32] https://xss.as/threads/139109/post-986703/a11fe4ae01fe3bd1cc99e66c4af9606f ; https://github.com/BlackTechX011/HacxGPT-Jailbreak-prompts
[33] https://www.catonetworks.com/blog/cato-ctrl-wormgpt-variants-powered-by-grok-and-mixtral/ ; https://xss.as/threads/119869/post-976858/889bd2450ec700d2af069c5f3c949ba7

5. Learning

Capability:

AI is an incredible tool for learning. Standard LLMs can answer questions quickly and deep research agents can search for source material. Some models may integrate custom data sets to enable fraud. Threat actors can use these tools to learn how to commit crimes or to research their targets, including individuals, software, and technical systems. Tools like WormGPT, or jailbreaks which use specially crafted prompts to avoid safety classifiers, enable threat actors to directly ask "How do I blackmail someone?", "How do I get started in fraud?", "How do I make a fake login page for a bank?, or "Tell me about vulnerabilities in industrial control systems"

Harm 1: Reducing Barriers to Entry for Crime

Threat actors big and small, use AI to level up their cybercrime. Whether using it to research a victims industry, online footprint, or software systems[34] or to learn how to carry out crime. When used for research it lowers barriers to entry for cyber crime and makes threat actors more effective more quickly. While this is most notably enabling threat actors new to cyber crime it is also used by state-sponsored groups[35].

[34] https://cdn.openai.com/threat-intelligence-reports/5f73af09-a3a3-4a55-992e-069237681620/disrupting-malicious-uses-of-ai-june-2025.pdf

[35] https://www.securityweek.com/openai-says-iranian-hackers-used-chatgpt-to-plan-ics-attacks/

Addendum 2: Glossary

- **AI Agent:** An AI system that can perform tasks autonomously or semi-autonomously, including planning, decision-making, and using software tools. Malicious use includes automating scams, reconnaissance, or attacks.
- **Computer Use Agent:** An AI system that mimics human computer use, such as browsing, filling out forms, or running applications. These can be abused to automate fraud or simulate human behavior online.
- **Evil GPT:** A nickname for language models modified or prompted to produce harmful or illegal outputs. Often created via jailbreaking or fine-tuning for use in scams, harassment, or hacking.
- **Faceswap:** An AI technique that replaces one person's face with another in images or video. Can be used for impersonation, misinformation, or non-consensual explicit content.
- **Fine-Tuning:** Training an existing AI model on specific data to adjust its behavior. In malicious use cases, this includes stolen data, explicit images, or criminal content.
- **Jailbreak:** A method for bypassing an AI model's safety restrictions (typically with specially crafted prompts) to generate prohibited outputs like instructions for illegal activity.
- **Know your Customer (KYC)**: A set of processes used by financial institutions and regulated businesses to verify the identity of their clients. KYC helps prevent fraud, money laundering, and other illegal activities by requiring customers to provide personal information and documentation before accessing services.
- **Nudifying:** The use of AI to digitally remove clothing from a photo, creating fake nude images. Often used for extortion, harassment, or intimidation.
- **Romance Scams:** Fraud involving fake romantic relationships used to manipulate victims for money or sensitive information.
- **Sextortion:** Blackmail involving threats to release sexual images or content unless demands are met, often including money or more explicit material.
- **Voice Clone:** AI-generated speech that replicates a person's voice from audio samples. Can be abused for impersonation, scams, or fraud.
- **World Models:** AI systems that simulate how the physical world works. These can be used for planning, decision-making, or malicious actions like physical intrusion or infrastructure attacks.

Mr. BIGGS. Thank you very much.
Mr. Venske, you are recognized for your five minutes.

STATEMENT OF CODY VENZKE

Mr. VENZKE. Chair Biggs, Ranking Member McBath, and the Members of the Subcommittee, thank you for the opportunity to testify today on behalf of the American Civil Liberties Union.

I will address two issues this morning: First, it is crucial that our response to criminal uses of artificial intelligence adhere to the Constitution, civil rights, and civil liberties. Second, efforts by Congress and the administration must not inadvertently open the door for AI abuses such as through a moratorium on State regulation of AI or continuing consolidation of Federal data. With appropriate measures, Congress can ensure that AI is safe, effective, and consistent with our rights and liberties.

First, Congress' measures to address criminal AI must comport with the Constitution, civil liberties, civil rights, and privacy. For example, traditional First Amendment activities do not lose their protection simply because artificial intelligence was used. Editorial content moderation using AI is not categorically exempted from the First Amendment's protections. Neither is commentary on politicians or candidates for office. Speech about politicians and candidates, in particular, lies at the heart of the First Amendment and enjoys special protection. Consequently, courts have readily and correctly overturned laws prescribing false speech about politicians and candidates. The emergence and use of AI does not change the core foundational Constitutional precepts.

Likewise, privacy concerns may arise from obligations imposed on platforms that host and distribute AI systems. Requirements or incentives to search users' communications, to restrict their publication of models, code, and data, to monitor a report their online activity or to prohibit or undermine encryption, all increase governmental surveillance and, in some circumstances may violate the Fourth Amendment. As the Committee considers legislation addressing criminal uses of AI, we urge you to ensure that speech, privacy, and other important civil liberties are protected.

Second, the recently rejected AI moratorium would have dramatically increased the risk of AI harms including criminal and fraudulent activity. Similarly, the consolidation of Federal data is creating enormous risk of AI harms. The moratorium that was included in versions of the reconciliation package was sweeping, preempting State laws and local regulations that regulate AI for 10 years. Although the moratorium included limited exemptions for some generally applicable laws, serious questions about the scope and workability of those exemptions remain. For example, dozens of States have passed laws regulating deepfake, nonconsensual intimate imagery often by amending existing statutes to clarify their application to generative AI.

Similarly, Tennessee's ELVIS Act extends legal protection to a person's voice including a simulation of the voice. It is not clear if such laws with their express application or clear intent to apply to AI qualify as generally applicable. Moreover, in many instances addressing AI's harm requires legislating specifically on AI. Establishment of an AI moratorium will jeopardize these efforts giving

bad actors a blank check. As Ranking Member McBath recognized, 17 Republican Governors and members of both parties in both chambers of Congress oppose the moratorium before Congress stripped it from the reconciliation package in a 99 to one vote in the Senate.

The more immediate concern, consolidation of Federal data creates a platform for super charged AI driven surveillance. While data consolidation sharing could potentially improve governmental operations and limited circumstances, efficiency should not be elevated over robust protection of our privacy, otherwise consolidation could risk the creation of vast and unaccountable surveillance platform, capable of tracking citizens' activities, movements, and associations. Such a platform would be readily analyzable by large language models, machine learning, and other AI systems such as black box fleecing algorithms used by Federal law enforcement to ingest governmental data and predict who is likely to commit crimes.

Data consolidation could lead to biometric information gathered by Federal law enforcement or during air travel, being readily accessible by other agencies. Records related to firearms might be accessible across the Federal Government and IRS data reflecting contributions to organizations like the ACLU, the NAACP, the NRA, or The Heritage Foundation could be accessible to Federal law enforcement without meaningful process. It is essential for Congress to block the reaction of centralized government dossiers on each of us.

Thank you for the opportunity to testify before this Subcommittee and I look forward to your questions.

[The prepared statement of Mr. Venzke follows:]

STATEMENT OF

Cody Venzke

Senior Policy Counsel

National Political Advocacy Division

American Civil Liberties Union

For a Hearing on

"Artificial Intelligence and Criminal Exploitation: A New Era of Risk"

Before the

United States House of Representatives

House Judiciary Committee

Subcommittee on Crime and Federal Government Surveillance

July 16, 2025

Chairman Biggs, Ranking Member McBath, and members of the Subcommittee: Thank you for the opportunity to testify today on behalf of the American Civil Liberties Union (ACLU) regarding the risks posed by the rapidly advancing frontier of artificial intelligence (AI). The risk posed by malicious actors' use of artificial intelligence is real. The increasing prevalence of AI in our lives is accompanied by corresponding potential for harm. However, it is crucial that our response to those risks be consistent with civil rights and civil liberties. Likewise, Congress should ensure that the legislation it passes and the actions of the Administration do not open the door for malicious actors to abuse AI. Congress has already stepped up in this regard, ensuring that a "moratorium" on state regulation of AI was not included in the recent reconciliation package.

In addition to the threats posed by malicious actors, governmental use of AI carries concomitant risks. As with the private sector, governmental use of AI is pervasive, cutting across federal law enforcement, governmental benefits, and national security. Although some use cases may make governmental programs and services more effective and more efficient, the risks AI poses in this domain may, in some instances, be even more significant and consequential than those that arise from malicious actors outside the government. Indeed, as President Trump recognized during his first term, federal use of AI must "foster[] public trust and confidence while protecting privacy, civil rights, civil liberties, and American values."[1]

This statement addresses five issues:

- Congress should ensure that efforts to address malicious uses of artificial intelligence comport with civil rights and civil liberties
- Current rollbacks of AI safeguards threaten safety, civil rights and civil liberties
- AI is being deployed across governmental programs, including federal law enforcement, without adequate safeguards, and in some places, in violation of existing statutory or regulatory safeguards on governmental use of data collected on individuals
- The revised Office of Management and Budget Memorandum is an important milestone for safe, effective governmental AI, but key shortcomings should be addressed
- Congress should address the civil rights impacts of artificial intelligence in traditionally protected sectors

---

[1] Exec. Order No. 13960 of December 3, 2020, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," 85 Fed. Reg. 78939 (Dec. 8, 2020); *see also* Exec. Order No. 13859 of February 11, 2019, "Maintaining American Leadership in Artificial Intelligence," 84 Fed. Reg. 3967 (Feb. 14, 2019) (recognizing that federal uses of AI mut protect "economic and national security, civil liberties, privacy, and American values").

I. Congress Should Ensure that Efforts to Address Malicious Uses of Artificial Intelligence Comport with Civil Rights and Civil Liberties

As Congress contemplates measures to address the use of AI in criminal, malicious, or fraudulent activity, it must ensure that those measures comport with basic Constitutional precepts of due process, privacy, civil rights, and civil liberties. This means protecting "open" AI to the extent possible, respecting the use of AI in First Amendment activities, and minimizing surveillance.

Preserving AI "Openness": Recent concerns have focused on how "open" AI might contribute to AI misuse.[2] "Openness" in AI is a gradient, encompassing a broad range of formats, from the availability of downloadable models to publicly available model weights and fully "open" models with publicly available code, weights, and data.[3] Consequently, "openness" should always be discussed with reference to the components of the AI system that are being made widely available — such as the model weights, architecture or coding, or training data. Each degree of openness may further civil rights goals of transparency and explainability, especially when bolstered by additional protections as necessary.

As others have observed, "Widely available model weights enable external researchers, auditors, and journalists to investigate and scrutinize foundation models more deeply," including to assess harms to marginalized communities, by better understanding the relationship among the parameters evaluated by the model, especially in the context of sample data used to derive the weights.[4] Additional degrees of "openness" can further goals around transparency and accountability.

Relatedly, there is little evidence to show that "open" AI systems meaningfully increase risks of harms from AI.[5] Consequently, policymakers should resist impulses to cut off the development of "open" AI systems that do not appreciably increase AI risks.

Protecting First Amendment Activities: Similarly, as generative AI raises new concerns, policymakers should be cognizant that traditional First Amendment activities do not lose their protections simply because a new tool such as artificial

---

[2] *See* National Telecommunications & Information Administration, Dual-Use Foundation Models with Widely Available Model Weights Report (2024), https://www.ntia.gov/programs-and-initiatives/artificial-intelligence/open-model-weights-report [hereinafter "NTIA Report"].
[3] David Gray Widder et al., *Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI*, SSRN at 4 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4543807.
[4] Sayash Kapoor et al., *On the Societal Impact of Open Foundation Models*, arXiv at 4-5 (2024), https://arxiv.org/abs/2403.07918.
[5] NTIA Report at 36-37.

intelligence was used.[6] Thus, editorial content moderation using AI and algorithmic systems is not categorically exempted from First Amendment protections.[7] And critically, neither is commentary on politicians or candidates for office.[8]

Speech about politicians and candidates lies at the heart of the First Amendment and enjoys special protection.[9] The Supreme Court has emphasized, "Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution."[10] Consequently, "The First Amendment affords the broadest protection to such political expression in order 'to assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'"[11]

Courts have readily overturned laws proscribing false speech about politicians and candidates, including on grounds that the laws are content discriminatory and that they lack narrow tailoring.[12]

For example, one court overturned a law punishing "derogatory" political speech, stating, "Under this statute, speakers may lie with impunity about businesspeople, celebrities, purely private citizens, or even government officials so long as the victim is not currently a" candidate.[13] "That is textbook content discrimination," subject to the highest levels of First Amendment scrutiny.[14] Laws seeking to limit AI-generated speech about politicians and candidates will likely raise the same concerns.

Of course, defamation, fraud, and child sexual abuse material are well-recognized exceptions to the First Amendment that apply equally to speech generated using AI, but many "deepfake" proposals extend beyond the traditional bounds of those

---

[6] *Cf.* Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 793 (2011); Anderson v. City of Hermosa Beach, 621 F.3d 1051, 1061–62 (9th Cir. 2010).
[7] Moody v. NetChoice, 603 U.S. 707, 731-742 (2024).
[8] Kohls v. Bonta, 752 F. Supp. 3d 1187, 1193 (E.D. Cal. 2024).
[9] Grimmett v. Freeman, 59 F.4th 689, 695 & n.8 (4th Cir. 2023).
[10] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 347 (1995).
[11] *Id.* (quoting Buckley v. Valeo, 424 U.S. 1, 14–15 (1976)); *accord* Roth v. United States, 354 U.S. 476, 484 (1957).
[12] Grimmett v. Freeman, 59 F.4th 689, 694 (4th Cir. 2023); Susan B. Anthony List v. Ohio Elections Comm'n, 45 F. Supp. 3d 765, 775 (S.D. Ohio 2014), aff'd sub nom. Susan B. Anthony List v. Driehaus, 814 F.3d 466 (6th Cir. 2016) ("While knowingly false speech may be an element of fraud or defamation, false political speech by itself does not implicate 'important private interests.' . . . As a result, knowingly false political speech does not fall entirely outside of First Amendment protection, and any attempt to limit such speech is a content-based restriction, subject to close review."); *accord* 281 Care Comm. v. Arneson, 766 F.3d 774 (8th Cir. 2014); *see also* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 57 (1988); New York Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964).
[13] Grimmett v. Freeman, 59 F.4th 689, 694 (4th Cir. 2023)
[14] *Id.*

exceptions or selectively regulate political speech.[15] Such proposals are likely to trigger rigorous judicial review.

Minimizing Surveillance: Finally, in efforts to mitigate criminal uses of AI, policymakers may consider imposing obligations on platforms that host and distribute AI models, weights, and tools. In considering that approach, policymakers should be cognizant of users' privacy rights. Privacy concerns may be triggered by requirements or incentives to search users' communications, monitor their online activity, restrict their publication of models, code, and data, report their activity to federal agencies, or to prohibit or undermine encryption. Those requirements undoubtedly increase governmental surveillance of private parties and, in some circumstances, may violate the Fourth Amendment.[16]

II. Current Rollbacks of AI Safeguards Threaten Safety, Civil Rights and Civil Liberties

Despite the concern about criminal uses of AI, some efforts by the Administration and Congress may either exacerbate those harms or hamper efforts to address them, including on matters within this Committee's jurisdiction.

a. A Federal Moratorium on State Regulation of AI Would Exacerbate the Risk of AI Harms

First, the ten-year "moratorium" that was included in earlier drafts of the recently enacted reconciliation package would have dramatically increased the risk of harms by artificial intelligence, including by criminal and fraudulent activity. The "moratorium" was publicly opposed by key members of both parties in the House, as well as by 17 Republican governors, before being defeated 99-1 in the Senate. The defeat of the moratorium underscored a bipartisan understanding that excluding states from AI regulation would be simply handing a blank check to bad actors.

Because some supporters of a moratorium have stated their goal of finding another legislative vehicle to enact a moratorium during this Congress, it is important for this Committee to understand the dangers of a moratorium in its various iterations. One component of the House reconciliation package would have imposed a ten-year "moratorium" on enforcement of state or local laws regulating AI. The moratorium was sweeping, affecting laws "regulating artificial intelligence models, artificial intelligence systems, or automated decision systems." Although the moratorium included limited exceptions for some state and local laws, serious questions arose

---

[15] United States v. Alvarez, 567 U.S. 709, 719 (2012) (false speech within traditional exceptions to the First Amendment may be regulated).
[16] United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010);

about the scope of those exceptions. In particular, the draft passed by the House would not have exempted laws unless it met three requirements:[17]

- The law's purpose is to remove AI barriers or use AI to streamline zoning, licensing, or similar activities;
- The law does not impose "any substantive design, performance, data-handling, documentation, civil liability" or other obligations on AI unless it is a "generally applicable" law that applies to all technology evenly; "and"
- The law does not impose a fee or bond unless the fee or bond is reasonable and applies to all technology evenly.

The requirements were conjunctive, meaning a law would be exempted *only* if it satisfied all three. Few laws would have been able to meet that bar. Further, even after Senate redrafting clarified the relationship among these prongs, serious questions persisted over what laws *exactly* qualify as "generally applicable."

Those are serious questions and ambiguities that even further refined drafting will not be able to resolve. For example, dozens of states have passed laws regulating nonconsensual intimate imagery (NCII) created by generative AI, often by simply amending an existing NCII statute to clarify that it applies to images created with generative AI.[18] It is not clear if such laws, which specify their application to generative AI, qualify as "generally applicable." Similarly, Tennessee's ELVIS Act amends its existing right of publicity statute to extend to a person's "voice" — a concern that has risen in prominence due to AI voice-cloning technology.[19] The definition of "voice" specifically encompasses a "simulation." Although the amendment does not specify any type of AI technology, its intent to address emerging AI technology is clear.

Moreover, in many instances, addressing AI's harms requires legislating specifically on AI. Establishment of an AI moratorium will jeopardize these efforts, giving bad

---

[17] Cody Venzke et al., *Expert Perspectives on 10-Year Moratorium on Enforcement of US State AI Laws*, Tech Policy Press (May 23, 2025), https://www.techpolicy.press/expert-perspectives-on-10-year-moratorium-on-enforcement-of-us-state-ai-laws.

[18] *E.g.*, 84 Del. Laws ch. 479 (2024) (HB 353), https://legis.delaware.gov/BillDetail?LegislationId=141103; Md. Laws ch. 219 (2024) (SB 360E), https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0360?ys=2025RS; N.Y. Laws Ch. 513 (2023) (S1042A), https://www.nysenate.gov/legislation/bills/2023/S1042/amendment/A; N.Y. Laws Ch. 58, part MM, subpart A, sec. 3 (2024) (A8808), https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=A08808&term=2023&Summary=Y&Actions=Y&Text=Y;

[19] Tenn. Pub. Ch. No. 588 (2024) (HB 2091), https://publications.tnsosfiles.com/acts/113/pub/pc0588.pdf; Sy Damle et al, *The ELVIS Act: Tennessee Shakes Up Its Right of Publicity Law and Takes On Generative AI*, Latham & Watkins Client Alert (Apr. 8, 2024), https://www.lw.com/en/offices/admin/upload/SiteAttachments/The-ELVIS-Act-Tennessee-Shakes-Up-Its-Right-of-Publicity-Law-and-Takes-On-Generative-AI.pdf.

actors a blank check. Recognizing this, Congress stripped the moratorium from the reconciliation package in a 99-1 vote in the Senate. This Committee should oppose any renewed efforts to try to enact a moratorium preempting state laws.

b. Consolidation of Federal Databases Will Require Facilitation by Artificial Intelligence and Raises Questions About Compliance with Legal Requirements

The Administration's efforts to consolidate federal data also pose risk of AI harms, including supercharged domestic surveillance. On March 20, 2025, President Trump issued Executive Order 14243, titled "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos."[20] The Executive Order directs federal agencies to facilitate the sharing and consolidation of agency records, with the stated goal of combating waste and fraud. However, the broad and unregulated access to sensitive data not only violates privacy obligations but also risks the creation of a database that contains a single, searchable profile of every American, without transparency or clear legal limits. And while data consolidation and sharing could potentially improve certain government operations in limited circumstances, it must be done in a way that does not elevate efficiency over robust privacy protection. Otherwise, this could risk the eventual creation of a vast and unaccountable surveillance system capable of tracking every citizen's activities, movements, and associations, readily analyzable by large language models, machine learning, and other AI systems.

Implementation of the Executive Order raises significant concerns about compliance with legal restrictions on federal and state data. For example, the Privacy Act of 1974,[21] prohibits disclosure of records from any federal agency's "system of records," including to other agencies. The law includes a variety of exceptions, such as disclosures to agency employees for "performance of their duties" and for "routine uses" that are compatible with the original purpose of collection and published in the Federal Register. Similarly, the Social Security Act requires states participating in Medicaid to develop plans to ensure that Medicaid data is disclosed only for four purposes "directly related to the administration" of the Medicaid program:[22] (1) establishing eligibility; (2) determining the amount of medical assistance; (3) providing services for beneficiaries; and (4) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan. Broad-based sharing and consolidation of federal records defies those restrictions.

---

[20] Exec. Order No. 14243 of March 20, 2025, 90 Fed. Reg. 13681 (Mar. 25, 2025).
[21] 5 U.S.C. § 552a.
[22] 42 U.S.C. § 1396a(a)(7) (requiring the state plan to limit disclosures to those "directly connected with administration" of the state plan); 42 C.F.R. § 431.301–02.

A similar program was pursued by the Department of Defense in the early 2000s. The Total Information Awareness (TIA) program was designed to mine vast amounts of personal data from a variety of sources, including commercial databases, travel records, and financial transactions, in the name of national security. This program was loudly criticized across the political spectrum, and in response to efforts led by Senator Wyden and with the support of Senator Grassley, Congress halted funding for TIA. Mission creep made even a purportedly limited database a serious threat to civil rights and civil liberties. As Senator Grassley observed then: "Like many people, I have been concerned that this program could be used to invade the privacy of Americans by snooping around in our bank accounts, personal Internet computers, phone records and the like."[23]

Senator Grassley ultimately concluded in opposing the program: "Without appropriate oversight and accountability standards, Total Information Awareness could infringe on [Constitutional] rights. Snooping around by the feds cannot go unchecked."[24] More than 20 years later, the new threat is from a potentially far more expansive and invasive program.

Building a centralized system for federal data, as envisioned under the Executive Order, creates similar risks, and threatens to create a single point of vulnerability where personal information could be exploited for improper surveillance or wrongful government action. Functionally this data consolidation will enable centralized dossiers on nearly everyone in the United States that would leap over the firewalls around agency data that prevent misuse and abuse.

Consolidating such data could lead to biometric information gathered by one law enforcement agency, or during air travel, being merged with or easily accessible to other law enforcement agencies, and the reverse could also be true. Records related to firearms, maintained by federal firearms licensees, the FBI, or the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), might be reviewed by other federal entities, potentially to assess eligibility for government programs such as Social Security or Medicare — and the FBI and ATF could similarly access Social Security and Medicare records, including medical files. Likewise, IRS data reflecting contributions to organizations like the ACLU, NAACP, NRA, or the Heritage Foundation could become accessible to law enforcement.

Such broad data sharing risks violating well-established privacy safeguards, and it is essential for Congress to actively monitor these practices and ensure that these

---

[23] Declan McCullagh, *Republican Senator Slams Database Plan*, CNET (Jan. 22, 2003), https://www.cnet.com/tech/services-and-software/republican-senator-slams-database-plan/.
[24] Sen. Chuck Grassley, *Pentagon Snoops Need Congressional Leash* (Jan. 31, 2003), https://www.grassley.senate.gov/news/news-releases/pentagon-snoops-need-congressional-leash.

privacy laws are upheld while blocking the creation of a centralized government dossier on nearly every individual in this country. Because significant amounts of federal data are being shared with components of the Departments of Justice and Homeland Security under this Committee's jurisdiction, the Committee has oversight authority to ensure that data sharing is not being used to build a centralized surveillance platform. If necessary, this Committee can — and should — consider legislation to limit agencies' collection, purchase, use, and consolidation of data.

c. Directives to Deploy AI, Including in Hiring, Raise Serious Concerns About Safety and Civil Rights

Efforts across the government to implement AI at a breakneck pace could mean that federal AI outstrips nascent safeguards, such as the "risk management practice" developed by the Office of Management and Budget (OMB).[25]

For example, the President directed the Assistant to the President for Domestic Policy and the Office of Personnel Management, in conjunction with OMB and the Department of Government Efficiency (DOGE), to develop a "Federal Hiring Plan."[26] The hiring plan was directed to "integrate modern technology to support the recruitment and selection process" of federal employees.[27] The subsequent Federal Hiring Plan directs agencies to adopt skills-based assessments and "rigorous candidate ranking."[28] Although the Hiring Plan contemplates use of validated assessments through USA Hire, it also permits use of "agency-developed and off-the-shelf assessments."[29] Under the plan and OPM's forthcoming "rule of many," agencies will be able to set "cut scores" for their assessment, based on analysis data, business necessity, or set numbers or percentages of applicants.[30] We fear these measures will lead to unproven products like gamified assessments, automated video interviews, and chatbots.[31] These technologies have been repeatedly demonstrated to lead to discriminatory harms, and many workers have reported that today's digital-application platforms are particularly confusing,

---

[25] OMB's safeguards for federal uses of AI are discussed in Section IV of this statement.
[26] Exec. Order No. 14170 of January 20, 2025, 90 Fed. Reg. 8621 (Jan. 30, 2025).
[27] *Id.* sec. 2(b)(vi)
[28] Vince Haley & Charles Ezell, Memorandum to Heads and Acting Heads of Departments and Agencies at 7 (May 29, 2025), https://chcoc.gov/sites/default/files/Merit%20Hiring%20Plan%205-29-2025%20FINAL.pdf.
[29] *Id.* at 17.
[30] *Id.* at 7.
[31] Olga Akselrod & Ricardo Mimbela, *The Long History of Discrimination in Job Hiring Assessments*, ACLU (May 30, 2024), https://www.aclu.org/news/racial-justice/the-long-history-of-discrimination-in-job-hiring-assessments.

inaccessible, and opaque.[32] Without safeguards, this influence will translate directly into real world harms.

Moreover, DOGE appears to be actively deploying AI across federal agencies, potentially without adhering to safeguards for federal uses of AI, such as OMB's risk management practices. For example, AI has been deployed at the federal Department of Education,[33] with access to grant and financial information, resulting in "a massive firehose of data being sent to [an] AI company's servers."[34] Similarly, data analytics and AI company Palantir has been contracted to build a portal to make highly protected IRS data available across the federal government.[35] This rapid deployment raises the risk that AI is being used without sufficient safeguards. This Committee should exercise its oversight authority, including by holding hearings if warranted, to determine how AI is being applied in agencies within the Committee's jurisdiction.

III. AI Is Being Deployed Across Governmental Programs, Including Federal Law Enforcement

In addition to being cognizant of the harms that may stem from criminal exploitation of AI, the Committee should use its jurisdiction to investigate and address harms that may arise from the government's own use of artificial intelligence in governmental benefits and administration, federal law enforcement, and national security.

a. Federal Law Enforcement

Artificial intelligence has become commonplace in federal law enforcement. The uses of AI in law enforcement are diverse, ranging from facial recognition technology to algorithmic decision-making and predictive policing. Despite the multiplicity of use cases across law enforcement, AI consistently undermines due process protections and poses threats to the public trust by exacerbating existing

---

[32] Olga Akselrod & Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired*, ACLU (Aug. 23, 2023), https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired.

[33] Hannah Natanson, *Elon Musk's DOGE Is Feeding Sensitive Federal Data Into AI to Target Cuts*, Washington Post (Feb. 6, 2025), https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education.

[34] *Ranking Member Connolly Demands Answers After Reports DOGE is Feeding Americans' Private Data Into Unapproved AI Systems, Using AI to Slash Programs*, House Committee on Oversight and Government Reform Democrats (Mar. 12, 2025), https://oversightdemocrats.house.gov/news/press-releases/ranking-member-connolly-demands-answers-after-reports-doge-feeding-americans.

[35] Makena Kelly, *Palantir Is Helping DOGE With a Massive IRS Data Project*, Wired (Apr. 11, 2025), https://www.wired.com/story/palantir-doge-irs-mega-api-data/.

disparities, operating without transparency, and being deployed without adequate auditing or risk mitigation.

i. Facial recognition technology

One example of such a tool is facial recognition technology (FRT). The ACLU has consistently taken the position that the use of face recognition technology poses serious threats to civil liberties and civil rights, making it dangerous both when it fails and when it functions.[36] Accordingly, the ACLU has repeatedly called for a federal moratorium on the use of facial recognition by federal law enforcement.[37]

The use of FRT is pervasive. For example, the Chairman of this Subcommittee recently sought information from the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) on ATF's use of FRT to identify gun owners.[38] As Chairman Biggs noted, the use of FRT by federal agencies, including ATF, is marred by a lack of oversight and transparency, as federal agencies failed to systematically track their use of FRT systems. Often, federal use of FRT was not accompanied by established guidance or policies addressing civil rights and civil liberties.

Similarly, the Federal Bureau of Investigation has closely tied FRT to its larger domestic surveillance apparatus. The FBI employs facial recognition technology in intelligence gathering and national security contexts, including identifying individuals connected to open assessments — preliminary investigations that don't require any suspicion of wrongdoing — as long as they serve a recognized purpose such as preventing crime or terrorism.[39]

---

[36] ACLU, Re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Executive Order 14074, Section 13(e)), (Jan. 19, 2024), https://perma.cc/3FLB-Q54Z. ACLU, Response to U.S. Commission on Civil Rights Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology (April 8, 2024) https://www.aclu.org/wp-content/uploads/2024/04/ACLU-Comment-to-USCCR-re-FRT-4.8.2024.pdf.

[37] More than 20 jurisdictions — including Boston; Minneapolis; Pittsburgh; Jackson, Mississippi; San Francisco; King County, Washington; and the State of Vermont — have enacted legislation halting most or all law enforcement or government use of face recognition technology. Others, such as the states of Maine and Montana, have enacted significant restrictions on law enforcement use of the technology. And law enforcement agencies in jurisdictions such as New Jersey and Los Angeles have prohibited use of Clearview AI, an FRT vendor that markets a particular privacy-destroying system built on a database of tens of billions of non-consensually collected faceprints.

[38] Letter from Hon. Andy Biggs, Chairman, Subcommittee on Crime and Federal Government Surveillance, & Warren Davidson, Member of Congress, to Hon. Kash Patel, Acting Director, Bureau of Alcohol, Tobacco, Firearms, and Explosives (Mar. 27, 2025), https://biggs.house.gov/sites/evo-subsites/biggs.house.gov/files/evo-media-document/biggs-letter-to-atf-acting-director-patel-re-atf-improper-facial-recognition-technology.pdf.

[39] House Oversight and Reform Committee: Facial Recognition Technology - Ensuring Transparency in Government Use (June 4, 2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, FBI), https://perma.cc/H56E-MUN3; U.S. Senate AI

This lack of oversight and transparency poses significant risks to civil rights and civil liberties. As an initial matter, facial recognition technology is often unreliable and frequently produces possible matches that are incorrect.[40] Even in best case scenarios, these systems are not designed to deliver definitive identifications. Instead, they generate what is essentially an "algorithmic best guess" of who a person might be, which often results in incorrect matches.[41] A variety of factors influence how accurate facial recognition technology is, including how the algorithm was trained, the composition of the image database it is matched against, and characteristics of the input image, such as the lighting, angle, and image quality.[42]

The most troubling issue is that facial recognition technology systems consistently demonstrate disproportionately high error rates when applied to people of color and women, compared to white men.[43] Related technologies that analyze faces to assign genders to a face can disproportionately fail for gender non-conforming individuals.[44] Efforts to test and improve the accuracy of facial recognition technology above some threshold rest on extremely shaky ground because current FRT accuracy tests do not reflect real-world conditions or the human factors in FRT use.

As explained in a 2022 report from the Georgetown Center on Privacy and Technology, existing FRT accuracy tests do not control for the many variables characterizing real-world law enforcement uses of FRT.[45] A study designed to assess accuracy rates of FRT algorithms *as actually used in police investigations* would need to account for both algorithmic and human factors in the FRT search process, as well as the tremendous variability in the quality of probe images, which often feature low resolution, poor lighting, and other deficiencies. But existing studies do not do so. For example, real-world uses of FRT searches will present dozens or

---

Insight Forum: National Security (Dec. 6, 2023) (statement of Patrick Toomey, Deputy Director, National Security Project, ACLU), https://perma.cc/C34K-8ECW.

[40] Because FRT systems conducting one-to-many searches are generally configured to produce multiple possible matches, even when the algorithm identifies a true match, it will also necessarily generate numerous false matches.

[41] Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, The New Yorker (Nov. 13, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence; *see also Facial Recognition: Current Capabilities, Future Prospects, and Governance*, Nat'l Acad of Scis. at 48-49 (2024), https://perma.cc/K7PR-AJAS.

[42] *Facial Recognition: Current Capabilities, Future Prospects, and Governance* at 47.

[43] *Id.* at 24, 56–57.

[44] Morgan Klaus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, ACM Digital Library (2019), https://dl.acm.org/doi/10.1145/3359246.

[45] Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations*, Geo. L. Ctr. on Privacy & Tech at 15-16 (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.

hundreds of potential matches for a probe image;[46] human investigators must sift through the raft of potential matches to select leads for further investigation. As demonstrated by the known cases of misidentifications leading to wrongful arrests, that human review process is prone to error.[47]

Other human and technical factors further exacerbate the risk inherent in FRT. The probe image may be pixelated, grainy, taken from an angle, or with facial features obscured,[48] in contrast with the more ideal conditions used in laboratory tests. Humans must also select a similarity threshold for the FRT algorithm, which establishes cut-off of similarity for images in the dataset compared to the probe image. Choosing a lower threshold will lower the risk of missing a true match while raising the risk of overwhelming the examiner with false matches; a higher threshold will lower the number of false positives that are provided but increase the chance of missing a true match, which may have outsized impacts on different demographic groups.[49]

Predictably, police reliance on this technology has led to a number of wrongful arrests across the country.[50] Reflecting the demographic disparities in false-match rates from the technology, most of the people known to have been wrongfully arrested due to police reliance on incorrect FRT results are Black. This includes the ACLU's former client Robert Williams, who was wrongfully arrested by Detroit police in 2020 after police relied on an incorrect FRT result in a shoplifting investigation. But everyone is at risk. Just last year, a white Florida resident was wrongfully arrested after an incorrect FRT result led police in a city 300 miles from

---

[46] Dep. of Jennifer Coulson at 29, Williams v. City of Detroit, No. 21-cv-10827 (E.D. Mich.), ECF No. 60-2 (Michigan State Police analyst explaining that candidate list included 486 images generated by the FRT search).

[47] Clare Garvie, *A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations*, Geo. L. Ctr. On Privacy & Tech. at 22-24 (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations ("A wealth of psychology research demonstrates that overall, humans are not innately good at identifying unfamiliar faces."); *Facial Recognition: Current Capabilities, Future Prospects, and Governance*, Nat'l Acad. of Scis. At 61-63, 83-84 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

[48] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Geo. L. Ctr. on Privacy & Tech. (May 16, 2019), https://www.flawedfacedata.com.

[49] K.S. Krishnapriya et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race* 3, IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops (2019), https://arxiv.org/abs/1904.07325 ("A specified FMR [false match rate] is usually realized by different threshold values relative to the African-American and the Caucasian impostor distributions.").

[50] *See* Douglas MacMillan, David Ovalle & Aaron Schaffer, *Arrested by AI: Police Ignore Standards after Facial Recognition Matches*, Wash. Post (Jan. 13, 2025), https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition.

his home to charge him with luring or enticing a child.[51] Although police eventually admitted that the FRT result was wrong, it was too late to prevent the harms of being falsely accused of a reviled crime and held in jail.

Despite these significant shortcomings, facial recognition technology used by government agencies is on the rise. Most known deployments involve attempting to match individuals to still images or identifying them in photographs, often in criminal investigations. However, the prospect of continuous video surveillance using facial recognition is becoming more real, especially as federal agencies responsible for national and homeland security increasingly explore and adopt AI-powered facial recognition tools.[52]

Although use of FRT to identify or track people through real-time or stored video feeds has long remained taboo in American policing,[53] a recent Washington Post investigation revealed that the New Orleans Police Department has been secretly relying on a network of live FRT cameras that send real-time alerts to officers' phones when the cameras detect a purported match to someone on a privately assembled watch list.[54] In addition to critical risks of misidentifications and wrongful arrests from continuous untargeted FRT use, deploying FRT on a network of surveillance cameras enables automatic tracking of huge numbers of people as they go about their daily lives, raising acute constitutional concerns. Such surveillance threatens to chill the exercise of rights protected by the First Amendment, including the freedoms of speech, association, and of the press.

---

[51] Evan Dean, *AI Leads to Wrongful Arrest of Lee County Man*, Gulf Coast News (Feb. 11, 2025), https://www.gulfcoastnewsnow.com/article/ai-leads-to-wrongful-arrest-of-lee-county-man/63745255.

[52] See, e.g., ACLU, Comment re: DHS Information Collection Request (Dec. 6, 2021), https://www.aclu.org/documents/aclu-comment-dhs-st-information-collection-request-facial-recognition-and-artificial; see also GAO, Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections (GAO-22-106100) (June 29, 2022), https://perma.cc/9APH-CPUU (indicating that DOD, DHS, DOJ, and DOS had reported using facial recognition technology for national security and defense related purposes). Section 5708 of the FY2020 National Defense Authorization Act mandated that the Director of National Intelligence submit a report on the use of facial recognition technology. This report has never been made public despite it being required to have been submitted in an unclassified form.

[53] Even in jurisdictions that allow use of FRT to attempt to identify images of unknown suspects, continuous video FRT surveillance is prohibited. *See, e.g.*, Miami Police Dep't, Departmental Order 16, Chapter 4: Facial Recognition Technology, § 4.5.2(d), ("Facial recognition technology . . . shall not be used for . . . [m]onitoring persons in real time."); Detroit Police Dep't, Directive No. 307.5: Facial Recognition, § 3.2 ("Members shall not use Facial Recognition on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source."); Mont. Code Ann. § 44-15-104; Mass. Gen. Laws. Ann. ch. 6, § 220(a); Va. Code § 52-4.5(D); L.A. Cnty. Regional Identification System, Facial Recognition Policy ¶ E (Sept 1, 2021); Orlando Police Dep't Policy & Procedure 1147.2, Facial Recognition § 5.3 (June 6, 2022).

[54] Douglas MacMillan & Aaron Schaffer, *Police secretly monitored New Orleans with facial recognition cameras*, The Washington Post (May 19, 2025), https://www.washingtonpost.com/business/2025/05/19/live-facial-recognition-police-new-orleans/.

Further, the U.S. Supreme Court has made clear that using digital-age technologies to conduct pervasive surveillance of people's locations and movements implicates the Fourth Amendment.[55] A system that scans every face that passes by enables dangerous dragnet surveillance that is simply incompatible with our expectations in a free society.

And consequently, the ACLU continues to urge this Committee and Congress to enact a federal moratorium on the use of this technology in law enforcement, due to its inherent risk for civil rights and civil liberties. As an important step towards such a moratorium, we urge this Committee to schedule an oversight hearing on the use of facial recognition technology, and other AI, by federal law enforcement.

ii. Algorithmic Decision-Making & "Predictive Policing"

Law enforcement and the criminal legal systems also rely on algorithmic systems to make decisions about individuals or where to allocate policing resources. So-called "predictive policing" relies on technology that includes tools that are built using a wide array of inputs, including historical crime data, which are used to "to help decide where to deploy police" (place-based) or "to identify individuals who are purportedly more likely to commit or be a victim of a crime" (person-based).[56] Both person-based and place-based predictive policing tools raise serious civil rights and civil liberties concerns,[57] which arise in part due to the data used to build those systems.

To build these systems, developers generally train algorithms using datasets that may include historical crime data amassed by police departments over the course of many years, sometimes decades.[58] Those data sets reflect existing disparities in police practices, such as over-policing of Black and Brown communities. Alarmingly, some police departments train predictive systems on information collected from unlawful practices, such as arrest records legally mandated to be sealed. Building

---

[55] Carpenter v. United States, 585 U.S. 296 (2018).
[56] Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Justice (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
[57] *See, e.g.*, Kristian Lum & William Isaac, *To Predict and Serve?*, Royal Stat. Soc. (2016), https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x; Danielle Ensign et al., *Runaway Feedback Loops in Predictive Policing*, Procs. of Machine Learning Rsch. (2018), https://proceedings.mlr.press/v81/ensign18a/ensign18a.pdf; Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 NYU L. Rev. (2019), https://nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/.
[58] *See* Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Justice (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

models off data that inherently contain bias results in biased tools creates a feedback loop that serves to further oppress Black and brown communities.

Several examples of flawed predictive systems stand out:

- **PATTERN:** The PATTERN risk assessment developed by the U.S. Department of Justice is used to inform programming and release decisions for individuals incarcerated in federal facilities. PATTERN scores can be calculated by adding up whole numbers based on roughly a dozen pieces of information about a person, and these scores may be calculated using paper-based forms or processes.[59] While a tool like PATTERN may appear to be simple, the tool was developed using statistical modeling techniques, including "machine learning boosted regression procedures,"[60] and it is used in ways that, like seemingly more complex AI systems, raise serious concerns about transparency, accuracy, and fairness.[61] These concerns arise from how PATTERN purported to measure likelihood of recidivism, which it based on data regarding likelihood of *rearrest*.[62] That distinction is critical. Overwhelming research has demonstrated that arrest is more reliably a measure of policing practices and priorities than actual crime, making arrest a racially-biased proxy for recidivism.[63] For example, when it comes to traffic stops — the most common form of interaction between police and the public — study after study has demonstrated that police engage in persistent racial discrimination when conducting stops, frisks, searches and arrests.[64]

---

[59] *See* Federal Bureau of Prisons, *PATTERN Risk Assessment,* https://www.bop.gov/inmates/fsa/pattern.jsp (last visited November 27, 2023).
[60] *See 2021 Review and Revalidation of the First Step Act Risk Assessment Tool*, National Institute of Justice at 16 (2021), https://nij.ojp.gov/library/publications/2021-review-and-revalidation-first-step-act-risk-assessment-tool.
[61] *See Formal Statement of the American Civil Liberties Union For a Stakeholder Engagement Session on First Step Act Implementation*, ACLU (Sept. 27, 2022), https://www.aclu.org/wp-content/uploads/document/ACLU_PATTERN_Public_Comment.pdf; Coalition Letter on the Use of PATTERN Risk Assessment in Prioritizing Release in Response to the COVID-19 Pandemic, ACLU (April 3, 2020), https://www.aclu.org/letter/coalition-letter-use-pattern-risk-assessmentprioritizing-release-response-covid-19-pandemic; ACLU, Comment Letter to Department of Justice on PATTERN First Step Act (Sept. 3, 2019), https://civilrights.org/resource/comment-letter-to-department-of-justice-on-pattern-first-step-act/.
[62] U.S. Department of Justice, 2021 Review and Revalidation of the First Step Act Risk Assessment Tool, available at https://nij.ojp.gov/library/publications/2021review-and-revalidation-first-step-act-risk-assessment-tool (December 2021).
[63] *See, e.g.,* American Civil Liberties Union, *A Tale of Two Countries: Racially Targeted Arrests in the Era of Marijuana Reform*, ACLU (2020), https://www.aclu.org/publications/tale-two-countries-racially-targeted-arrests-era-marijuana-reform; Lum & Isaac, *To Predict and Serve*, In Detail (2018), https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2016.00960.x.
[64] *See* Baumgartner et al., *Targeting young men of color for search and arrest during traffic stops: evidence from North Carolina*, Politics, Groups, and Identities (2016), https://fbaum.unc.edu/articles/PGI-2016-Targeting.pdf; Pierson et al., *A large-scale analysis of racial*

Moreover, a large percentage of arrests do not result in convictions.[65] Taken together, this evidence suggests multiple, fundamental issues with using rearrests as a proxy for recidivism.

- **Patternizr:** The New York City Police Department (NYPD) has been using millions of sealed arrest records in more than a dozen interconnected technologies including one predictive policing tool known as Patternizr.[66] Patternizr is a machine-learning model created by the NYPD that is trained on complaint and arrest reports that were generated between 2006 and 2015.[67] The corpus of data used to train Patternizr includes sealed records[68] and data from the height of the NYPD stop-and-frisk program, which targeted Black and Latino people and was ruled unconstitutional.[69] Hundreds of thousands of people stopped under that racially biased program were arrested,[70] often on specious allegations later dismissed, thus creating records that may well populate Patternizr. Querying Patternizr by submitting a new crime complaint will return additional, purportedly related complaints,[71] effectively suggesting specific individuals for detectives to investigate — meaning a person might find themselves suspected of a crime based solely on Patternizr's selection of their sealed arrest record in response to a detective's query. A class action filed by the Bronx Defenders challenging the NYPD's use of sealed arrest records — including in Patternizr — as a contravention of New York law is ongoing.[72]
- **Geolitica:** Geolitica (formerly known as PredPol) is a leading place-based predictive policing company that purports to help officers identify high-priority areas for patrol.[73] Those recommendations, however, reflect existing disparities in policing practices and create a feedback loop that will perpetuate them. As computer scientist Suresh Venkatasubramanian succinctly stated, "If you build predictive policing, you are essentially sending

---

disparities in police stops across the United States, Nature Human Behavior (2020); https://www.nature.com/articles/s41562-020-0858-1.

[65] For a discussion of the data from various jurisdictions about what percentage of arrests result in convictions, see Ames Grawert, *Brennan Center's Public Comment on the First Step Act's Risk and Needs Assessment Tool*, Brennan Center for Justice (2019); https://www.brennancenter.org/our-work/research-reports/brennan-centers-public-comment-first-step-acts-risk-and-needs-assessment.

[66] *See id. See also*, *R.C. v. City of New York*, No. 153739/2018, 2021 WL 4427369 (N.Y. Sup. Ct. Sept. 27, 2021) (granting preliminary injunction).

[67] Alex Chohals-Wood & E.S. Levine, *A Recommendation Engine to Aid in Identifying Crime Patterns* (Mar. 29, 2019), https://nparikh.org/assets/pdf/sipa6545/week10-police/policing/nypd-patternizr.pdf.

[68] *See* Complaint at 2, *R.C. v. City of New York*, 153739/2018 (N.Y. Sup. Ct. Apr. 4, 2018).

[69] *Floyd v. City of New York*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

[70] *See id.* at 573.

[71] *Id.* at 6–8.

[72] *Id.*

[73] *Data-Driven Community Policing*, Geolitica (2023), https://geolitica.com/public-safety.

> police to certain neighborhoods based on what they told you — but that also means you're not sending police to other neighborhoods because the system didn't tell you to go there. . . If you assume that the data collection for your system is generated by police whom you sent to certain neighborhoods, then essentially your model is controlling the next round of data you get."[74]

Predictive policing tools are necessarily built on top of historical data—and the history of policing is a deeply racist one.[75] Historical crime data is not an objective history of all crime: it does not capture unreported crime, officer discretion in investigations and arrests, or the series of racist decisions that lead to a conviction in some cases and not others. Analyzing police behavior and crime data have revealed racial disparities in every stage of the criminal process.[76] To paint the picture, a Black person is more than twice as likely to be arrested than a white person, and five times more likely to be stopped without cause than a white person.[77] AI trained on that history will undoubtedly replicate it, exacerbating and automating discriminatory harms.

While many of the studies of the harms caused by AI in "predictive policing" have focused on harms related to race, the increasing use of machine learning and "black box" AI could very well mean that it becomes increasingly difficult to understand what factors the systems are relying on.[78] Consequently, there is no reason to believe that AI in predictive policing can be applied fairly and accurately, even in contexts unrelated to race. Models might rely on factors ranging from gun

---

[74] Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm Is Fundamentally Flawed*, Vice (Feb. 14, 2019), https://www.vice.com/en/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed.

[75] *See* Connie Hassett-Walker, *The Racist Roots of American Policing: From Slave Patrols to Traffic Stops*, The Conversation (June 2, 2020), https://theconversation.com/the-racist-roots-of-american-policing-from-slave-patrols-to-traffic-stops-112816.

[76] Ezekiel Edwards, *Predictive Policing Software Is More Accurate at Predicting Policing Than Predicting Crime*, ACLU (Aug. 31, 2016), https://www.aclu.org/news/criminal-law-reform/predictive-policing-software-more-accurate ("Time and again, analysis of stops, frisks, searches, arrests, pretrial detentions, convictions, and sentencing reveal differential treatment of people of color. From racial bias in stops and frisks in New York, Boston, and Baltimore, to unwarranted disparities nationwide in arrests of Blacks and whites for marijuana possession (despite comparable usage rates), to disparities in the enforcement of minor offenses in Minneapolis, New Jersey, and Florida, as sure as the sun rises police will continue to enforce laws selectively against communities of color.").

[77] Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.*, MIT Tech. Rev. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice.

[78] Dominic Weiss, *Inhuman Reason: Predictive Policing Algorithms and the Fourth Amendment*, ABA Criminal Justice Magazine (Jan. 30, 2025), https://www.americanbar.org/groups/criminal_justice/resources/magazine/2025-winter/predictive-policing-algorithms-fourth-amendment/.

ownership to marital status — or simply being the victim of a crime[79] — could similarly result in the wrongful targeting of police resources based on a machine's guess of who might commit a crime. At its core, predictive policing is inconsistent with due process.

b. Governmental Benefits and Administration

AI is actively being deployed in basic governmental operations. These AI systems affect everything from governmental benefits to child welfare programs and public housing:

- **Medicaid:** Idaho's Department of Health and Welfare was employing algorithmic systems to determine benefits for federally funded Medicaid programs.[80] Although the system cut some individuals' benefits by as much as 30 percent, officials were unable to explain why determinations were reached, and litigation by ACLU of Idaho revealed that the system was implemented without meaningful safeguards. The algorithmic system was implemented without notice, and the State of Idaho and its private vendor attempted to hide its functioning behind trade secrets claims.[81] The ACLU of Idaho eventually prevailed in court and learned that Idaho's system was "a set of formulas in a fairly basic Microsoft Excel spreadsheet," which computed each person's benefits in "hidden cells," leaving state officials unable to explain how or why it reached its benefits determinations.[82] Despite its outsized impact on individuals' rights, Idaho's algorithmic system lacked critical safeguards, based on underlying models that "Department staff had just brainstormed," but "never validated, standardized, or audited the instrument."[83]
- **Allegheny Family Screening Tool:** An ACLU and Human Rights Data Analysis Group audit of an algorithmic risk-scoring system used to inform child welfare decision-making in Allegheny County, Pennsylvania highlighted several ways in which the algorithm's design and deployment could enable algorithmic bias.[84] The risk-scoring system could potentially

---

[79] J. Justin Wilson, *Case Closed: Pasco Sheriff Admits "Predictive Policing" Program Violated Constitution*, Institute for Justice (Dec. 4, 2024), https://ij.org/press-release/case-closed-pasco-sheriff-admits-predictive-policing-program-violated-constitution.
[80] Testimony of Ritchie Eppink, Hearing AI in Government Before the S. Comm. On Homeland Security & Government Affairs (May 16, 2023), https://www.hsgac.senate.gov/hearings/artificial-intelligence-in-government.
[81] *Id.* at 3.
[82] *Id.*
[83] *Id.*
[84] Marissa Gerchick et al., *How Policy Hidden in an Algorithm is Threatening Families in This Pennsylvania County*, ACLU (Mar. 14, 2023), https://www.aclu.org/news/womens-rights/how-policy-hidden-in-an-algorithm-is-threatening-families-in-this-pennsylvania-county; Marissa Gerchick et al.,

disproportionately flag Black families and families with disabilities for investigation. The audit highlighted the system's use of existing government databases, including county child welfare, juvenile probation, and behavioral health records. Problematically, those databases reflect the lives of those who have more contact with government agencies and systems shaped by historical and ongoing discrimination — not necessarily those who pose greater "risk" to their children. Additionally, the outcome the tool predicts is the risk of child removal by the County, based on its historical practices. Because government databases, including those regarding child removal statistics, reflect systems shaped by historical and ongoing discrimination, using them to identify the characteristics of households more likely to have a child removed means selecting from a pool of factors that over-represents some groups of people and underrepresents others.

- **Tenant Screening:** "[C]rime-fighting grants" provided through the U.S. Department of Housing and Urban Development have been used by local housing authorities to deploy AI-powered surveillance.[85] For example, in "rural Scott County, Va., cameras equipped with facial recognition [technology] scan everyone who walks past them, looking for people barred from public housing."[86] Numerous other uses of facial recognition and similar technology in federally funded housing have been well documented.[87] Likewise, public housing authorities may rely on algorithmically driven tenant screening, including criminal background checks used as a prerequisite for public housing, often with discriminatory effects on over-policed populations.[88]

The Devil is in the Details: Interrogating Values Embedded in the Allegheny Family Screening Tool, ACLU (2023), https://www.aclu.org/the-devil-is-in-the-details-interrogating-values-embedded-in-the-allegheny-family-screening-tool. Allegheny County and its Department of Human Services receive federal funds. *DHS Funding*, Allegheny County (2023), https://www.alleghenycounty.us/Human-Services/About/Funding-Sources.aspx; *County Of Allegheny*, TAGGS (2023), https://taggs.hhs.gov/Detail/RecipDetail?arg_EntityId=swAAHUn5jiXXGX5RfqF%2Fmg%3D%3D.

[85] Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing*, Washington Post (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing.

[86] *Id.*

[87] *Id.*; Dan Bateyko, *Taken for Granted: Where's the Oversight of AI and Federal Funding?*, CDT (Aug. 7, 2023), https://cdt.org/insights/taken-for-granted-wheres-the-oversight-of-ai-and-federal-funding.

[88] DeMetria McCain, Principal Deputy Assistant Secretary for Fair Housing and Equal Opportunity, U.S. Department of Housing and Urban Development, Memorandum on Implementation of the Office of General Counsel's Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions 2 (June 10, 2022), https://www.hud.gov/program_offices/fair_housing_equal_opp/fheo_guidance ("[H]ousing providers sometimes utilize third-party companies to independently screen and reject applicants using algorithms that may contain racial or other prohibited bias in their design."); *see* Comments of the

The potential risks posed by these systems to public trust, safety, privacy, civil rights, and civil liberties can be commensurate to the risks posed by exploitative or malicious uses of AI.

c. National Security

Over four years ago, the National Security Commission on Artificial Intelligence (NSCAI) issued a sweeping report that made clear U.S. intelligence agencies like the NSA, CIA, FBI, and others are pursuing "ubiquitous AI integration in each stage of the intelligence lifecycle."[89] Intelligence agencies are seeking to use AI to help select surveillance targets, identify people whose communications are intercepted, and analyze the vast amounts of data they collect.[90] Despite transparency commitments by ODNI and the agencies it oversees, the public knows little about how these AI applications are impacting people in the United States. For example, the National Security Agency has used AI "for a very long time" to support its intelligence-gathering activities, and today it is one of many spy agencies seeking to integrate AI across its activities.[91] AI may be used at the NSA for selecting targets for intelligence,[92] monitoring social media,[93] risk assessments, and watch listing.[94]

IV. The Revised Office of Management and Budget Memorandum Is an Important Milestone for Safe, Effective Governmental AI, But Key Shortcomings Should Be Addressed

Initial efforts to address the potential harms from federal uses of AI are underway. Under the Trump Administration, the Office of Management and Budget (OMB) revised crucial guidance for federal agencies' use of AI to ensure American leadership in both AI innovation and AI effectiveness, trustworthiness, and safety. This guidance, Memorandum M-25-21,[95] is built on principles of transparency and

---

ACLU, Tenant Screening Request for Information, Docket No. FTC-2023-0024 (May 30, 2023), https://www.aclu.org/wp-content/uploads/2023/07/2023.05.30-ACLU-Comment-to-FTC-CFPB-Tenant-Screening-RFI.pdf (describing private uses of algorithmic tenant screening).

[89] NSCAI Final Report at 110, https://perma.cc/FQ5H-ZGEH.

[90] *Id.* at 108–10, 143–45.

[91] *GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT*, NSA (Sep. 21, 2023), https://perma.cc/97GE-4ULZ.

[92] *See* NSCAI Final Report at 109, 112.

[93] Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, VICE (May 17, 2023), https://www.vice.com/en/article/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees/.

[94] DHS, *Artificial Use Case Inventory—Customs and Border Protection*: *Port of Entry Risk Assessments*, https://perma.cc/RCP2-VZWJ (last visited June 13, 2024); DHS, *2020–2021 Data Mining Report*, DHS at 26 (2022), https://perma.cc/9K6P-GUHG.

[95] Memorandum for the Heads of Executive Offices and Agencies, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," M-25-21 (Apr. 3, 2025),

American values, including protecting civil rights and civil liberties, established by Executive Orders and legislation during the first Trump Administration.

During his first term, President Trump directed that "[a]gencies must [] design, develop, acquire, and use AI in a manner that fosters public trust and confidence while protecting privacy, civil rights, civil liberties, and American values."[96] OMB expounded on those principles in an earlier memorandum to direct agencies to "consider in a transparent manner the impacts that AI applications may have on discrimination."[97] In the same memorandum, OMB recognized that "transparency and disclosure can increase public trust and confidence in AI applications" and that disclosures "should be written in a format that is easy for the public to understand and may include identifying when AI is in use."[98]

Ultimately, Congress enshrined these principles of public trust, transparency, civil rights, and civil liberties into law. The Advancing American AI Act mandates that each agency "prepare and maintain an inventory of the artificial intelligence use cases of the agency."[99] Similarly, the AI in Government Act of 2020 required OMB to provide guidance on identifying "best practices for identifying, assessing, and mitigating any discriminatory impact or bias on the basis of any classification protected under Federal nondiscrimination laws, or any unintended consequence of the use of artificial intelligence."[100]

a. Key Provisions of M-25-21 Will Help Ensure Federal AI Is Safe, Trustworthy, and Protective of Civil Rights and Civil Liberties

Memorandum M-25-21 is the latest iteration of efforts to foster public trust in federal uses of AI. Several key strengths of the Memorandum will help ensure that federal AI is safe, trustworthy, and protective of civil rights and civil liberties:

- **Public Use Case Inventories:** Transparency around federal uses of AI was foundational for AI policy during the first Trump administration. OMB's

---

https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf [hereinafter Memorandum M-25-21].

[96] Exec. Order No. 13960 of December 3, 2020, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," 85 Fed. Reg. 78939 (Dec. 8, 2020); *see also.* Exec. Order No. 13859 of February 11, 2019, "Maintaining American Leadership in Artificial Intelligence," 84 Fed. Reg. 3967 (Feb. 14, 2019) (recognizing that federal uses of AI mut protect "economic and national security, civil liberties, privacy, and American values").

[97] Memorandum for the Heads of Executive Offices and Agencies, "Guidance for Regulation of Artificial Intelligence Applications," M-21-06, sec. 7 (Nov. 17, 2020) [hereinafter M-21-06].

[98] *Id.*, sec. 8.

[99] Advancing American AI Act, Pub. L. No. 117-263, div. G, tit. LXXII, subtit. B, sec. 7225, 136 Stat. 2395, 3672 (2022), https://www.congress.gov/bill/117th-congress/house-bill/7776/text.

[100] AI in Government Act of 2020, Pub. L. No. 116-260, div. U, tit. I, sec. 104(a)(3), 134 Stat. 1182, 2287 (2020), https://www.govinfo.gov/content/pkg/PLAW-116publ260/pdf/PLAW-116publ260.pdf.

2020 Memorandum on AI emphasized that "the continued adoption and acceptance of AI will depend significantly on public trust and validation," and consequently urged agencies to prioritize public participation and to provide information to the public on agencies' uses of AI.[101] Similarly, President Trump's 2020 Executive Order on artificial intelligence established the first framework for AI use-case inventories,[102] a requirement that was later incorporated into the Advancing American AI Act.[103] Memorandum M-25-21 preserves many key components of the public use case inventories by requiring agencies to publicly document each "use case" of AI,[104] including compliance with the Memorandum's risk management practices.[105]

- **Robust Risk Management Practices:** The core of Memorandum M-25-21 is a series of "risk management practices" to mitigate risks posed by certain "high-impact" uses of AI.[106] Crucially, these risk management practices include pre-deployment testing that reflects "expected real-world outcomes" and conducting AI impact assessments.[107] The impact assessments must address the quality and appropriateness of the AI system's data and capability, potential impacts on privacy, civil rights, and civil liberties, and the result of an independent review.[108] The AI must be monitored for adverse impacts throughout its life cycle, including functions that "may violate laws governing privacy, civil rights, or civil liberties."[109]
- **Broad Scope of "High-Impact" AI:** The Memorandum's core "risk management practices" apply to "high-impact" AI. "High-impact" AI is any AI that "serves as a principal basis for decisions or actions with legal, material, binding, or significant effect" on key areas of life: "civil rights, civil liberties, or privacy"; "access to education, housing, insurance, credit, employment, and other programs"; "access to critical government resources or services"; "human health and safety"; "critical infrastructure or public safety"; or "strategic assets or resources," including classified information.[110] Any AI that meets that definition must comply with the risk management practices

---

[101] M-21-06, secs. 1-2.
[102] Exec. Order No. 13960, sec. 5.
[103] Pub. L. No. 117-263, div. G, tit. LXXII, subtit. B, sec. 7225, 136 Stat. 2395, 3672 (2022), https://www.congress.gov/bill/117th-congress/house-bill/7776/text.
[104] Memorandum M-25-21, sec. 3(b)(v). As described below, the Department of Defense and the intelligence community are exempt from providing public AI use case inventories.
[105] *Id.* sec. 4(a)(i).
[106] Memorandum M-25-21, sec. 4(b).
[107] *Id.* sec. 4(b)(i).
[108] *Id.* sec. 4(b)(ii), (B), (C), (F).
[109] *Id.* sec. 4(b)(iii).
[110] Memorandum M-25-21, sec. 5.

unless an exception applies. In addition, several uses are *presumed* to be high-impact and subject to the risk management practices, including:[111]

- blocking, removing, hiding, or limiting the reach of protected speech;
- using risk assessments and facial recognition in law enforcement;
- adjudicating requests for critical federal services, processes, and benefits, including loans and access to public housing, continued
- eligibility benefits; and,
- determining the terms of employment.

- **AI Under Human Oversight:** The Memorandum appropriately recognizes that although AI may not independently make decisions or fully automate a task, it may nonetheless be "a principal basis" for consequential decisions or actions that carry risks to rights and safety. For example, the Memorandum recognizes that AI may be "high-impact" "whether there is or is not human oversight for the decision or action."[112] Similarly, the Memorandum emphasizes that "risks" arising from AI may occur whether "the AI merely informs the decision or action, partially automates it, or fully automates it."[113] This approach corresponds to how AI is actually used in practice, where AI often works in tandem with human decision-makers, rather than fully replacing them.

  For example, one law enforcement agency used an algorithmic systems to predict who was likely to predict future crimes,[114] including by drawing grades and abuse histories from the local school district's education records.[115] That algorithmic score was based not just on individuals' own criminal records, but merely being suspected of a crime, serving as a witness to a crime, or being a victim of a crime.[116] Officers then used the algorithmic output to identify individuals for harassment, seeking "to get them to move away or go to prison," including by getting more than a dozen individuals evicted from their homes.[117] Although humans made the ultimate decisions,

---

[111] *Id.* sec. 6.
[112] Memorandum M-25-21, sec. 4(a).
[113] Memorandum M-25-21, sec. 7.
[114] J. Justin Wilson, *Case Closed: Pasco Sheriff Admits "Predictive Policing" Program Violated Constitution*, Institute for Justice (Dec. 4, 2024), https://ij.org/press-release/case-closed-pasco-sheriff-admits-predictive-policing-program-violated-constitution.
[115] Neil Bedi & Kathleen McGrory, *Pasco's Sheriff Uses Grades and Abuse Histories to Label Schoolchildren Potential Criminals*, Tampa Bay Times (Nov. 19, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data.
[116] *Florida Parents Partner with IJ to Shut Down Dystopian "Predictive Policing" Program*, Institute for Justice (Mar. 10, 2021), https://ij.org/case/pasco-predictive-policing.
[117] Bedi & McGrory, *supra* note 115.

the algorithm's output was crucial to causing the harm, placing individuals in the crosshairs for governmental abuse.

Similarly, one predictive model used in colleges and universities evaluates individual students' likelihood of academic success and assigns them a corresponding "risk score." One investigation found the model's risk scores correlated with students' race, and in some cases, expressly incorporated it as a "high-impact predictor."[118] Academic advisors often review students' risk scores, and although the model did not independently make decisions about students, its scores might nonetheless "leave advisers with an immediate and potentially life-changing impression of students and their prospects within a given major."[119] Although AI did not make the final determination, its influence was significant, and the OMB Memorandum covers such scenarios.

b. Memorandum M-25-21 May Be Strengthened by Addressing Critical Shortcomings

Despite its strengths, the OMB Memorandum includes broad carveouts that threaten its efficacy in protecting the public's trust. As Congress and the Administration continue to improve governance of federal uses of AI, four key shortcomings should be addressed, either through legislation or working directly with OMB:

- **Bolstering Use Case Inventories:** The use case inventories may be further strengthened:
    - A previous iteration of the Memorandum required agencies to "*individually* inventory" each use case,[120] a requirement that was removed from Memorandum M-25-21. Individual documentation increases transparency, as it helps ensure that the public is aware of each AI system and avoids risks that crucial AI use cases would be obscured in aggregate reporting.
    - Further, the previous iteration of the Memorandum required that agencies not subject to the *individual* reporting requirement "still report and release aggregate metrics about such use cases that are otherwise within the scope of this memorandum, the number of such cases that impact rights and safety, and their compliance with" the

[118] Todd Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, The Markup (Mar. 2, 2021), https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success.
[119] *Id.*
[120] Memorandum for the Heads of Executive Offices and Agencies, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," M-24-10, sec. 3(a)(iv) (Mar. 28, 2024) (emphasis added) [hereinafter M-24-10].

Memorandum's risk management practices.[121] Aggregate reporting achieved at least some balance between the purported need for confidentiality around military or intelligence AI uses and the need for transparency.

  - Finally, OMB has not yet publicly released its instrument for agencies to report use cases, but reporting suggests that the updated instrument will no longer gather crucial information. Omissions include whether notice is provided to individuals, whether there is human oversight or an option for opt-out, and if systems have disparate impact on protected classes.[122] Although neither version of the Memorandum required protections such as notice or opt-out in every instance,[123] collating the availability of those rights is crucial for both Congressional and public oversight.

- **Failure to Include State-Administered Federal Programs:** The Memorandum currently applies only to federal agencies—namely, any "executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch," with a few enumerated exceptions.[124] The scope of Memorandum at the federal level is appropriately broad, reflecting the broad use of AI across the federal government. However, the Memorandum excludes state and local programs receiving federal assistance; this will leave many particularly dangerous uses of AI unregulated, and OMB, the Administration, and Congress should take steps to expand the scope of the memorandum's applicability to federally funded programs. The exclusion of federally funded programs is particularly pernicious because federal funds may help support uses of AI with significant impacts on rights and safety, such as the Allegheny Family Screening Tool described above or AI technologies procured with Department of Justice grants.[125]

---

[121] M-24-10, sec. 3(a)(v).
[122] Madison Alder & Rebecca Heilweil, *Trump White House Issues Internal Federal Guidance on AI Reporting*, FedScoop (July 1, 2025), https://fedscoop.com/trump-white-house-issues-internal-federal-guidance-on-ai-reporting.
[123] M-24-10, sec. 5(c)(v)(B), (F) (opt-out required "where practicable and consistent with applicable law and governmentwide guidance"); M-25-21, sec. 4(b)(vi)-(vii) (requiring human review, appeal, and feedback mechanisms "where appropriate").
[124] *See* 44 U.S.C. § 3502(1).
[125] Brandon Block, *Federal Aid Is Supercharging Local WA Police Surveillance Tech*, Crosscut Cascade PBS (July 26, 2023), https://crosscut.com/investigations/2023/07/federal-aid-supercharging-local-wa-police-surveillance-tech; Chris Baumohl, *Two Years In, COVID-19 Relief Money Fueling Rise of Police Surveillance*, EPIC (Mar. 9, 2023), https://epic.org/two-years-in-covid-19-relief-money-fueling-rise-of-police-surveillance; Anastasia Valeeva, Wihua Li & Susie Cagle, *Rifles, Tasers and Jails: How Cities and States Spent Billions of COVID-19 Relief*, The Marshall Project (Sept. 7, 2022), https://www.themarshallproject.org/2022/09/07/how-federal-covid-relief-flows-to-the-criminal-justice-

- **Carveouts for National Security and Law Enforcement:** The Memorandum contains several carveouts for national security, defense, and law enforcement. The Advancing American AI Act codifies some of these exceptions for the intelligence community and the Department of Defense.[126] But the Memorandum itself establishes an *additional* exception for "national security systems,"[127] which can include systems involving intelligence activities, cryptologic activities, and "command and control of military forces," among other things.[128] As described above, these use cases can impose some of the most significant risks to civil rights and civil liberties, and their wholesale exemption from safeguards — even basic transparency — will exacerbate those harms.

  The Memorandum suggests that these agencies' uses of AI are "governed through other policy,"[129] but that is a significant overstatement. The policy sources it identifies are largely general statements of principles without meaningful accountability mechanisms or binding rules. For example, ODNI's *Principles for Artificial Intelligence Ethics for the Intelligence Community* describes six high-level guidelines — including a commitment to be "transparent and accountable," but the public to date has seen little evidence of either.[130] The Defense Department has released a toolkit "to help DoD personnel design, develop, deploy, and use AI systems responsibly," but using the toolkit is voluntary.[131]

---

system; Brian Naylor, *How Federal Dollars Fund Local Police*, NPR (June 9, 2020), https://www.npr.org/2020/06/09/872387351/how-federal-dollars-fund-local-police; Matthew Guariglia & Dave Maass, *How Police Fund Surveillance Is Part of the Problem*, EFF (Sept. 23, 2020), https://www.eff.org/deeplinks/2020/09/how-police-fund-surveillance-technology-part-problem.

[126] Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7225(d), 7228, https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf. "Intelligence community" is defined by 50 U.S.C. § 3003(4), and includes the Central Intelligence Agency, the National Security Agency, and the Defense Intelligence Agency, among others. The Advancing American AI Act exempts the intelligence community from the Memorandum's minimum risk management practices and both the intelligence community and the Department of Defense from the use case inventories. *Id.*

[127] Memorandum M-25-21, sec. 1(c).

[128] 44 U.S.C. § 3552(b)(6).

[129] Memorandum M-25-21, sec. 1(c) n.8.

[130] Office of the Director of National Intelligence, *Intelligence Community Principles of Artificials* (2020), https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2020/3634-principles-of-artificial-intelligence-ethics-for-the-intelligence-community-1692377385.

[131] Department of Defense, *CDAO Releases Responsible AI (RAI) Toolkit for Ensuring Alignment with RAI Best Practices* (Nov. 14, 2023), https://www.defense.gov/News/Releases/Release/Article/3588743/cdao-releases-responsible-ai-rai-toolkit-for-ensuring-alignment-with-rai-best-p/.

Similarly, President Trump directed the National Security Advisor to review recently issued National Security Memoranda (NSM) and make recommendations for rescissions[132] — which could include the NSM governing AI used as a component of national security systems.[133] Whether that NSM has been recommended for rescission is not publicly known. Overall, the intelligence and defense agencies lack specific rules and safeguards for their AI systems, as well as clear processes to implement and enforce those rules.

- **Potential Failure to Include More Rudimentary Algorithms:** The Memorandum incorporates one federal definition of "artificial intelligence," codified in the John S. McCain National Defense Authorization Act.[134] That definition limits "AI" to systems that "learn," use "human-like perception, cognition, [or] planning," "think or act like a human," "approximate a cognitive task," or "act rationally."[135] The scope of this definition is ambiguous — it may include more rudimentary algorithmic systems such as the PATTERN decision-making algorithm or Idaho's Medicaid benefits algorithm, or it may be limited to more advance technologies such as machine learning. Although more advanced technologies may present emerging challenges, existing, simpler algorithmic systems already in place are actively affecting civil rights and civil liberties.

In addition to addressing these shortcomings in the OMB Memorandum, this Committee and Congress will play important roles in ensuring that the Memorandum's directives — and the Congressional directives that underly it — are carried out by executive agencies. Neither the Memorandum nor its underlying statutory requirements have enforcement mechanisms, and Congress consequently has the ultimate responsibility through its oversight and budget authority to ensure that the Memorandum's protections are realized.

This Committee in particular has authority to conduct hearings and other oversight to ensure that the exceptions in the Memorandum are not simply a blank check for surveillance abuses. This includes ensuring that federal law enforcement is adhering to the Memorandum's safeguards and that national security and

---

[132] Exec. Order No. 14148 of January 20, 2025, sec. 3(c), 90 Fed. Reg. 8237 (Jan. 28, 2025).
[133] White House, Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence (Oct. 24, 2024), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security.
[134] Pub. L. No. 115-232, § 238(g) (2019), https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[135] *Id.*

intelligence agencies have sufficient policies and practices in place to protect civil rights and civil liberties.

V. Congress and this Committee Should Address the Civil Rights Impacts of Artificial Intelligence in Traditionally Protected Sectors

In addition to addressing criminal uses of AI, Congress should address the potentially discriminatory effects of AI, especially when used in traditionally protected sectors like housing, employment, credit, and more. For example, employers are using large language models to evaluate applicants' resumes,[136] which are instances of foundation models to evaluate job applicants, and those technologies can unfairly advantage male candidates or de-preference first-generation college graduates and racial minorities.[137] Other AI-driven hiring technology such as gamified personality tests can be inaccessible to and discriminate against applicants with disabilities.[138]

Similarly, credit scoring systems are algorithmic models that attempt to predict a borrower's risk and how well that person is likely to repay their debt obligations. These systems typically generate a numerical score used to help creditors in the financial services system determine the creditworthiness of a consumer. They are often used as part of a lender's decisions on underwriting and pricing. Algorithmic credit scoring disproportionately disadvantages Black, Latino, and Native American consumers who have historically had less access to traditional credit than white consumers.[139] As Federal Reserve Vice Chair of Supervision Michael Barr stated, "Artificial Intelligence…relies on the data that is out there in the world and the data…is flawed. Some of it is just wrong. Some of it is deeply biased…Information we have on the Internet is imperfect…if you train a Machine Learning device, if you

---

[136] Leon Yin et al., *OpenAI's GPT Is a Recruiter's Dream Tool. Tests Show There's Racial Bias*, Bloomberg (Mar. 7, 2024), https://www.bloomberg.com/graphics/2024-openai-gpt-hiring-racial-discrimination/.

[137] Avi Asher-Schapiro, *AI is Taking Over Job Hiring, But Can It Be Racist?*, Thomson Reuters (June 7, 2021), https://www.reuters.com/article/global-tech-ai-hiring/analysis-ai-is-taking-over-job-hiring-but-can-it-be-racist-idUSL5N2NF5ZC/; Jeffrey Dastin, *Insight - Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, Thomson Reuters (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/.

[138] Lydia X.Z. Brown et al., *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?*, Center for Democracy & Technology (2020), https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination/.

[139] Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

train a Large Language Model on imperfect data, you're going to get imperfect results."[140]

Similar examples exist across traditionally protected sectors. Consequently, policymakers' efforts to combat harmful or exploitative AI should include mitigating discriminatory harms from AI, including requiring impact assessments, mitigation of harms, ongoing monitoring, and notice and appeal — many of the same requirements the Trump administration has implemented for federal uses of AI.

VI. Conclusion

Thank you for the opportunity to testify before this Subcommittee. As you consider how to meet the challenges of artificial intelligence, it is important that the Committee and Congress ensure that its response comports with civil rights and civil liberties, and that you exercise your oversight and legislative authority over other federal efforts such as the Administration's "information silos" Executive Order, as well as oppose any congressional AI "moratorium" preempting state laws, so as to not open the door to malicious uses of AI.

---

[140] *See* Federal Reserve Board of Governors Vice Chair Michael Barr, *Setting the Foundation for Effective Governance and Oversight: A Conversation with U.S. Regulators*, Responsible AI Symposium (Jan. 19, 2024), https://www.youtube.com/watch?v=HbM_zD0esDo.

Mr. BIGGS. Thank you, Mr. Venzke.
Now, Mr. Redbord, you are recognized for five minutes.

STATEMENT OF ARI REDBORD

Mr. REDBORD. Chair Biggs, Ranking Member McBath, the Members of the Subcommittee, my name is Ari Redbord and it is an honor to appear before you today on behalf of TRM Labs, where we work every day with law enforcement, financial institutions, and national security agencies to detect, investigate, and prevent illicit activity in the digital asset ecosystem.

Before joining TRM I spent about 11 years as a Federal prosecutor at the U.S. Department of Justice and later as an official in the U.S. Treasury Department's Office of Terrorism and Financial Intelligence.

In those roles and now at TRM I've seen one truth borne out time and time again: Criminals are often the earliest adopters of transformative technology. They were among the first to weaponize automobiles to move illicit goods across State lines, adopt pagers and cell phones to coordinate narcotics networks, utilize encrypted messaging apps to evade surveillance, and exploit cryptocurrencies to steal and transfer illicit proceeds at the speed of the internet. Now they are embracing artificial intelligence.

We are rapidly approaching a world in which the bottleneck for crime is no longer human coordination, but computational power. When the marginal cost of launching a scam, phishing campaign, or extortion attempt approaches zero, the volume of attacks, and their complexity will increase exponentially.

We are not just seeing more of the same. We are seeing new types of threats that weren't possible before AI, novel fraud typologies, hyper-personalized scams, deepfake extortion, and autonomous laundering. The entire criminal ecosystem is shifting. That is why today's hearing matters.

We must recognize that in the same way criminals are leveraging AI to disrupt and deceive law enforcement and national security agencies must be empowered to use AI to defend and respond. This is not optional. It is foundational to preserve public trust and the social contract itself. If adversaries are deploying large-scale AI-enabled crime with impunity, and if the public no longer feels that government can protect them, we risk a breakdown of that trust. The consequences are not just individual harms; they are systemic national security-level threats to our institutions and civic cohesion.

At TRM we see this shift every day. Through Chainabuse, our public scam reporting platform, we've tracked a 456-percent rise in AI-enabled scams, which often use deepfake technology, just in the last year. Ransomware actors are using AI to draft realistic phishing emails, identify vulnerable targets, and deploy malware that adapts to evade detection.

On the laundering side we are seeing bad actors use AI to automate and accelerate illicit money flows. We are also seeing fully autonomous fraud agents scraping personal data, launching scam campaigns, and even coordinating laundering operations. The most disturbing, we're seeing AI used to generate synthetic child sexual

abuse material, fake, but deeply harmful content traded online and weaponized in sextortion schemes.

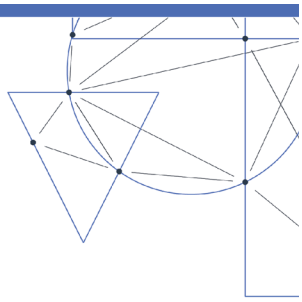
The solution to the criminal abuse of AI is not to ban or stifle the technology; it is to use it and use it wisely. We must stay a step ahead of illicit actors by leveraging the same innovations they use for bad, for good.

At TRM we integrate AI at every layer of our platform to combat crime using machine learning models and behavioral analytics to flag complex obfuscation techniques, trace illicit cryptocurrency transactions in real time, and identify emerging criminal typologies.

We are developing and deploying AI-powered defense agents at scale to map illicit networks, triage threats, and surface early warning signs. These operational tools are already being used in the field to help global law enforcement agencies move faster, trace complex laundering schemes, and target the highest-risk activity, often stopping criminal networks in their tracks before they can cause further harm.

The future of crime will be defined by AI, but so will the future of enforcement. With the right investment, collaboration, and technology we can meet this moment. Thank you again for the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Redbord follows:]



TRM

Testimony of Ari Redbord, Global Head of Policy, TRM Labs

Before the House Judiciary Subcommittee on Crime and Federal Government Surveillance
Hearing on: "Artificial Intelligence and Criminal Exploitation: A New Era of Risk"
July 16, 2025 | Room 2141, Rayburn House Office Building

Introduction

Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee, thank you for the opportunity to testify today on the urgent and evolving threat posed by artificial intelligence in the hands of criminal actors. I am honored to appear before you on behalf of TRM Labs, where we work every day with law enforcement, financial institutions, and national security agencies to detect, investigate, and prevent illicit financial activity in the digital asset ecosystem.

Before joining TRM, I spent about eleven years as a federal prosecutor at the US Department of Justice and later as an official in the US Treasury Department's Office of Terrorism and Financial Intelligence. In those roles — and now at TRM — I've seen one truth borne out time and again: criminals are often the earliest adopters of transformative technology. They were among the first to weaponize automobiles to move illicit goods across state lines, adopt pagers and cell phones to coordinate narcotics networks, utilize encrypted messaging apps to evade surveillance, and exploit cryptocurrencies to steal and transfer illicit proceeds at the speed of the internet. And now, they are embracing artificial intelligence (AI).

The FBI was created in 1908 — the same year the Model T was introduced — to pursue a new breed of criminal exploiting America's growing highway system to move faster and farther than ever before. Today, we find ourselves at a similar moment. Just as AI is revolutionizing medicine, education, and productivity, it is also unleashing an unprecedented era of speed, scale, and sophistication in criminal activity.

During my time at both DOJ and Treasury, I saw how quickly illicit actors adapted — using shell companies and darknet tools, exploiting gaps in global anti-money-laundering enforcement, and increasingly turning to cryptocurrency to move funds across borders. Now, at TRM, I see that adaptation accelerating. AI is removing human bottlenecks. It's not just enhancing traditional fraud — it's creating entirely new categories of criminal threat. And we are only beginning to understand the scale of this shift.

We are rapidly approaching a world in which the bottleneck for crime is no longer human coordination, but computational power. When the marginal cost of launching a scam, phishing campaign, or extortion attempt approaches zero, the volume of attacks — and their complexity — will increase exponentially. We're not just seeing more of the same; we're seeing new types of threats that weren't possible before AI. Novel fraud typologies, hyper-personalized scams, deepfake extortion, autonomous laundering — the entire criminal ecosystem is shifting.

That is why today's hearing matters. We must recognize that in the same way criminals are leveraging AI to disrupt and deceive, law enforcement and national security agencies must be empowered to use AI to defend and respond. This is not optional. It is foundational to preserving public trust — and the social contract itself. If adversaries are deploying large-scale, AI-enabled crime with impunity, and if the public no longer feels that government can protect them, we risk a breakdown of that trust. The consequences are not just individual harms — they are systemic, national security-level threats to our institutions and civic cohesion.

In the testimony that follows, I will walk through the state of AI-enabled crime across the ecosystem — from scams and fraud, to ransomware and cyberattacks, proliferation finance to disinformation and child exploitation. I will share what we are seeing at TRM through our investigations and data from Chainabuse, our open-source scam reporting platform. I will outline how TRM is leveraging AI to fight back. Finally, I will offer recommendations for how Congress can empower public-private collaboration, update legal frameworks, and help ensure that the tools of safety evolve as fast as the tools of harm.

The rise of AI-enabled crime and fraud

Artificial intelligence has revolutionized numerous industries, enhancing productivity and innovation at unprecedented speed. From increasing access to healthcare, to advanced climate modeling, to improving efficiency and security in workplaces — AI is enabling better, more sustainable outcomes across society.

However, this same transformative technology is also being leveraged for criminal purposes, posing significant threats to global security and societal stability. Malign actors are increasingly using AI to carry out hacks and fraud, create deepfakes for extortion and misinformation, and conduct cyberattacks at scale. As AI technology becomes more sophisticated, so too will the ways in which criminals exploit it for illicit gain.

TRM Labs has documented how AI removes the traditional bottlenecks that once constrained criminal activity. What used to require a team of humans — language translation, phishing email development, video editing, malware deployment — can now be accomplished by a single AI agent trained to operate at scale. Further, as at-home technology rapidly advances, powerful open-source LLMs and high-performance hardware will lower the barrier to entry and make it easier for an even wider range of illicit actors to operate independently without relying on expensive data centers.

We are watching, in real time, the industrialization of cyber-enabled crime.

How criminals are using AI

Criminals are increasingly incorporating AI into every stage of the illicit value chain. They use generative AI tools to write phishing emails in dozens of languages, create deepfake videos for extortion, develop synthetic identities for money laundering, and execute autonomous cyberattacks. TRM Labs categorizes this criminal adoption of AI across three phases:

- Horizon phase: AI use is possible but not yet operational. We see potential applications in areas like proliferation finance, where rogue states such as North Korea — already responsible for over USD 1.6 billion in crypto hacks in 2025 alone — could use AI agents to identify cybersecurity vulnerabilities or automate complex laundering schemes.

- Emerging phase: AI tools are deployed alongside human operators. This is where most AI-enabled fraud and ransomware operations exist today, with human actors directing large language models (LLMs) and deepfakes to scale their attacks. For example, the Internet Watch Foundation recently found over 3,500 AI-generated child sexual abuse images on a dark web forum, including content that overlaid children's faces onto adult actors. AI-generated deepfake voices are also increasingly used to impersonate executives or loved ones in extortion scams.

- Mature phase: AI dominates criminal activity. While no illicit domain has fully reached this point yet, we are moving toward it. AI systems are beginning to interface autonomously with email clients, databases, and cryptocurrency wallets, and they are being trained to optimize for outcomes such as revenue generation or influence. The recent "Terminal of Truths" case — in which an autonomous AI agent successfully interacted with users and bots to accumulate digital assets in a crypto economy — foreshadows this next frontier.

AI and ransomware

Ransomware actors are among those eagerly integrating artificial intelligence to enhance the efficiency, scale, and success rate of their attacks. AI-driven tools can generate highly personalized phishing emails and social engineering schemes that mimic trusted communications, often using deepfake audio or video to impersonate legitimate individuals.

On the technical front, ransomware developers are deploying AI to create polymorphic malware that continually adapts to evade detection by traditional security systems. Meanwhile,

machine learning algorithms can identify and prioritize high-value targets based on their financial standing, cybersecurity posture, and likelihood to pay — making ransomware attacks more strategic and profitable.

Looking ahead, AI is poised to further transform how ransomware proceeds are laundered through blockchain ecosystems. Autonomous laundering agents could execute complex schemes involving mixers, tumblers, and rapid cross-chain swaps, while leveraging decentralized finance (DeFi) protocols to layer transactions and obscure fund origins. Advanced AI models may also simulate legitimate transaction patterns to evade detection, dynamically adapting to new compliance tools and analytics.

These advancements create profound challenges for law enforcement, demanding greater investment in technology, expertise, and cross-jurisdictional coordination to counter rapidly evolving threats.

AI-enabled cyberattacks

Like ransomware attacks, the intersection of AI and cyberattacks has the potential to dramatically increase the scale, speed, and sophistication of exploits targeting critical infrastructure and financial systems. AI enables cybercriminals and nation-states to automate vulnerability scanning and craft highly targeted, devastating attacks with minimal human oversight.

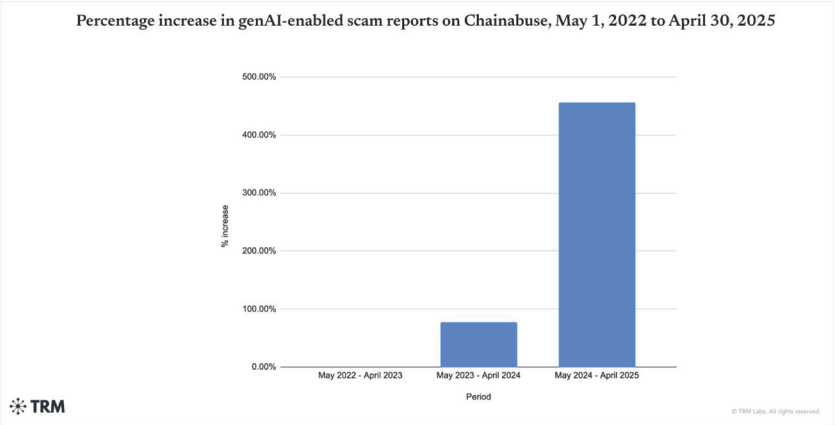
For instance, AI-powered tools can autonomously scan for weaknesses in critical sectors such as energy grids, hospitals, communication networks, and global financial systems. These vulnerabilities could include misconfigurations, unpatched systems, or gaps in security protocols, which can then be exploited with tailored malware or ransomware. Automating these processes significantly shortens the time it takes to breach security defenses, leading to a higher frequency and greater severity of cyberattacks. This presents serious risks, especially for sectors where AI-driven exploits could cause widespread disruption, affecting essential services and national security.

In the context of cryptocurrency and financial institutions, AI further enhances the ability of cybercriminals to identify and exploit weaknesses in security measures. By automating large-scale phishing campaigns and generating hyper-targeted exploits, criminals can more efficiently infiltrate systems and steal funds. The use of AI isn't just about increasing the volume of attacks; it amplifies their impact by enabling more precise and scalable efforts. Nation-state actors, like North Korean IT workers, could leverage AI to conduct automated scans of financial infrastructure, craft advanced exploits, and launder illicit funds,, making detection and

attribution significantly more challenging. As AI technology continues to evolve, so too must our cybersecurity infrastructure. Strengthening defenses and ensuring better coordination between private and public sectors is critical to countering these rapidly advancing threats.

AI-enabled scams

Perhaps the most widespread use of AI by criminals today is in perpetrating scams and fraud schemes against the public. In fact, data from Chainabuse — TRM Labs' open-source fraud reporting platform — shows that reports of generative AI-enabled scams between May 2024 and April 2025 rose by 456% compared to the same period a year earlier (which itself had seen a 78% rise over the year before). This explosion in readily available genAI tools has directly fueled a surge in AI-enabled fraud.

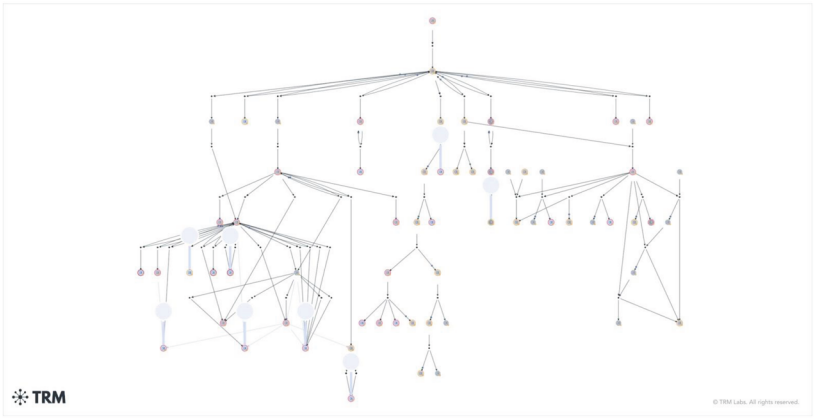


The most commonly reported type of AI-enabled scam is the deepfake cryptocurrency giveaway scam.

In this scheme, fraudsters create a genAI-powered twist on the classic "double-your-bitcoin" ploy. They compromise popular YouTube channels and use them to stream manipulated videos — often repurposing real interviews or speeches by prominent crypto figures such as Elon Musk, Ripple CEO Brad Garlinghouse, MicroStrategy CEO Michael Saylor, or Ark Invest CEO Cathie Wood — with scam websites and QR codes overlaid on the video. Using deepfake technology, the scammers alter these videos to make it appear that the celebrity is personally

endorsing a fraudulent giveaway or investment opportunity (for example, claiming they will double any cryptocurrency that users send in). These highly realistic streams are difficult to distinguish from authentic content, and they have tricked victims into sending millions of dollars in crypto to the scammers' addresses.

In June 2024, a Chainabuse report described a deepfake Elon Musk promoting a supposed AI-driven trading platform, which lured victims to scan a QR code causing the transfer of bitcoin. Funds from that address go to various destinations — but primarily to a few large exchanges, particularly MEXC. The scammers who defrauded this victim and others received at least USD 5 million between March 2024 and January 2025. TRM also observed small amounts of funds being sent to two darknet markets and a cybercrime entity.



TRM's Graph Visualizer has been used to map how scammers moved funds from these deepfake giveaway scams into exchange accounts like MEXC, illustrating the speed at which criminals can cash out once victims are duped

Deepfake impersonation scams and financial grooming

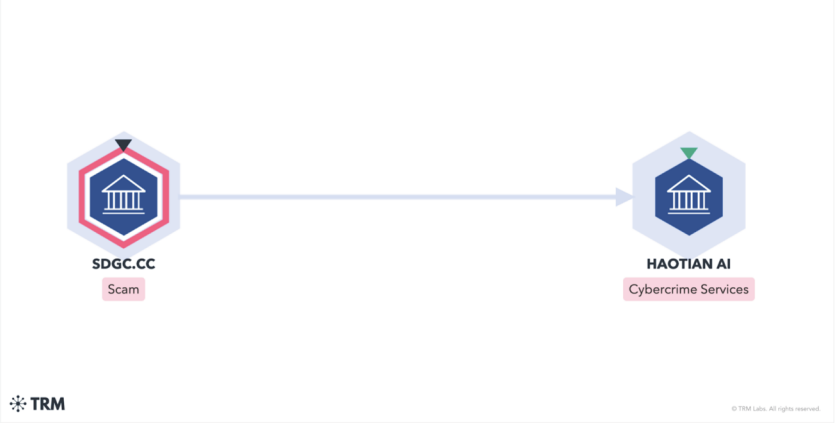
It is not only public figures who are being mimicked with deepfakes. Scammers are also using the technology to impersonate private individuals in real-time interactions.

Live deepfake technology (which can overlay one person's face onto another's in a live video call) means criminals no longer need large volumes of data to convincingly pose as someone

else. For example, in February 2024, a multinational company in Hong Kong was defrauded out of millions of dollars after an employee joined a video meeting with individuals pretending to be the company's executives. The scammers used real-time face- and voice-swapping AI tools to perfectly mimic the executives' appearance and speech, tricking the employee into authorizing a large transfer of funds.

In another common scheme, criminals clone the voice of a victim's family member or friend and call with a plea for help. The impostor (speaking in a loved one's voice) might claim to be in an emergency that requires immediate cash, or urge the victim to invest in a "can't-miss" opportunity that the friend purportedly has made money from. These AI-voice scams have led to heartbreaking losses, preying on victims' trust in those closest to them.

Deepfakes are also being used to bolster long-term fraud operations like romance or investment scams (so-called "pig butchering" schemes). TRM has identified cases where scammers utilize deepfake-as-a-service providers to enhance their deception during months-long grooming of victims. In one operation we traced, crypto payments from victims of romance/investment grooming scams were sent directly to platforms offering AI-generated video tools — strong evidence that organized scam networks are paying for deepfake technology as part of their criminal toolkit.



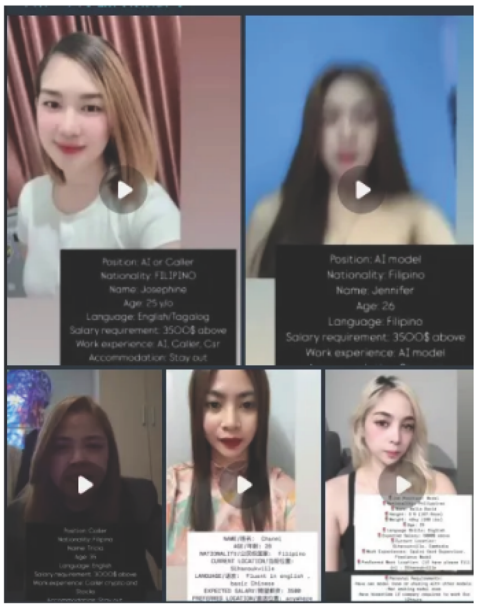
As shown in TRM Graph Visualizer, a scam entity sends funds to an AI-as-a-service entity, demonstrating scammers' willingness to pay for such services

Our investigators even encountered a scammer who appeared on a video call using a deepfake face overlay — evidenced by the person's unnatural-looking hairline and other digital artifacts. AI detection software later confirmed that the video was likely manipulated. This specific scam — along with related schemes tied to the same group — has defrauded victims of at least USD 60 million. The potential financial gains of these AI-augmented "pig butchering" scams are staggering.

Likely live deepfake used in financial grooming scam

As generative AI becomes more prevalent, the general public is also becoming more aware that video or audio evidence can be faked. To counter rising skepticism and appear legitimate, some scam operations are now blending real people with AI technology.

For example, TRM found evidence of women in Cambodia advertising their services via Telegram as "real face models" (as opposed to purely AI-generated personas) for scam call centers and online casinos. In these operations — when a victim insists on a live video chat — the scammers will have one of these human accomplices appear on camera. The "model" might then use a subtle deepfake filter to alter her appearance — making herself look more attractive or even to resemble a specific person — thereby ensuring the victim remains convinced of her identity.



Women claiming to have experience working as "AI" and "real face" models

By using a real human presence augmented with AI visuals, criminals are attempting to overcome victims' suspicion of fully synthetic media.

AI agents and fully automated fraud operations

Autonomous AI agents are emerging as a powerful force-multiplier for both legitimate and illicit operations. Unlike a standard AI tool that only responds to individual prompts, an autonomous agent can proactively carry out complex, multi-step tasks with minimal human oversight. In the hands of bad actors, these agents are being weaponized to industrialize fraud at a scale not previously possible. Criminals program AI agents to scrape public data (names, social media profiles, job roles, interests) and then craft hyper-personalized scam messages targeting those individuals.

They also use agents to automate mass outreach across email and social media platforms, deploy LLM-powered chatbots and fake "customer support" desks to lure victims — often

conversing with targets in their preferred language and cultural context to maximize credibility — and even run simulations to test different social engineering scripts in virtual environments to discover which are most convincing. Some fraudsters have begun using AI agents to manage the "back office" of their schemes as well: coordinating money laundering workflows, performing reconnaissance on law enforcement activity, and dynamically tweaking their scam strategies based on real-time feedback (for example, analyzing which phishing emails or scam websites are yielding the highest response rates from victims).

While many AI systems have built-in safeguards intended to prevent illicit use, criminals are finding ways around them. Through clever prompt engineering, offenders can manipulate AI models into revealing prohibited information or stratagems. For instance, a scammer might pose as an academic researcher or software developer when interacting with a large language model, coaxing it to provide step-by-step instructions for fraudulent schemes under the guise of legitimate inquiry.

This is no longer a theoretical concern — TRM researchers recently conducted an experiment by asking a supposedly restricted AI assistant how scammers might optimize their fraud operations using autonomous agents. Disturbingly, the tool responded with a surprisingly detailed set of illicit tactics, proving that current guardrails can often be circumvented. It is a stark reminder that as AI capabilities advance, so too must our vigilance against their malicious use.

AI in healthcare fraud

Earlier this month, the US Department of Justice (DOJ) announced the largest health care fraud takedown in US history — charging 324 defendants across 50 federal districts and 12 State Attorneys General's Offices for schemes involving more than USD 14.6 billion in intended losses. The operation targeted organized networks exploiting health care systems and patient data at scale, with a renewed emphasis on the convergence of health care fraud and modern financial laundering techniques, including the use of cryptocurrency.

In one of the cases, charged in the Northern District of Illinois, Pakistani executives were accused of using artificial intelligence to generate fake beneficiary consent recordings to bill Medicare fraudulently for USD 703 million in services. The scheme involved nominee-owned medical supply firms, AI-generated patient data, and offshore laundering. Approximately USD 44.7 million was seized across domestic and international accounts.

The use of AI to create fraudulent documents to bypass KYC and other ID verification checks

A growing example of criminal use of AI is the creation of fraudulent state-issued IDs designed to bypass Know Your Customer (KYC) and other identity verification checks. AI-powered services now generate highly convincing fake driver's licenses and passports, making it easier for criminals to evade detection during KYC procedures. These counterfeit documents can mimic real state-issued IDs from multiple countries, allowing criminals to pass through KYC checks on financial platforms, including cryptocurrency exchanges, banks, and other financial institutions, which typically rely on such IDs to confirm a user's identity.

Terrorist financiers could use fake IDs generated by AI to open accounts on financial platforms, allowing them to anonymously raise and transfer funds for illicit activities without detection. Similarly, money launderers and North Korean IT workers could exploit these fake identities to bypass KYC checks, moving stolen or sanctioned funds across borders while evading law enforcement tracking.

One notable example is OnlyFake, an AI-driven service that creates fake IDs for as little as USD 15, including passports and driver's licenses from 26 countries. These IDs have successfully bypassed KYC controls on cryptocurrency exchanges, banks, and other financial institutions, enabling cybercriminals and illicit actors to open accounts and move funds anonymously. As a result, fraudsters can exploit these fake documents to launder money and hide their activities.

To combat this, companies like Get Real Labs are developing tools to detect AI-generated fake IDs, helping to strengthen security and prevent criminals from circumventing identity verification processes.

Sextortion and synthetic CSAM

One of the most disturbing developments in AI-enabled crime is the use of artificial intelligence to produce fake sexual content for exploitation and blackmail — specifically, the creation of synthetic child sexual abuse material (CSAM).

In 2024, the Internet Watch Foundation found over 3,500 AI-generated images of child sexual abuse on a single dark web forum. These ranged from fully AI-synthesized depictions of abuse to "deepfake" creations where a real child's likeness was digitally mapped onto adult pornographic content. Such images and videos are traded in underground forums and shared via encrypted messaging apps, making it very difficult for authorities to track their spread or

identify the perpetrators. This is consistent with TRM's own investigations on the use of AI in creating CSAM.

AI-generated CSAM also exposes troubling gaps in our legal framework. Many child protection laws were written to address crimes involving real victims, and they struggle to account for imagery with no direct human victim that still causes harm. Even if no actual child was abused in the creation of an image, the material is psychologically damaging — both to the children whose likenesses are used and to society at large. Moreover, synthetic pornographic content is increasingly being weaponized in sextortion schemes: criminals threaten to distribute fake intimate images of someone (for instance, a doctored nude or a video that appears to show a minor) unless the victim pays them, often demanding cryptocurrency for its ease of transfer and anonymity.

Law enforcement must be equipped with the tools and authorities to investigate and prosecute these cases. That includes improved methods for tracing cryptocurrency flows associated with synthetic CSAM marketplaces and explicit legal provisions to charge those who produce or distribute AI-generated sexual abuse images — even if a loophole in current law means no real child was physically harmed.

Using AI to fight AI-enabled crime

The solution to the criminal abuse of AI is not to ban or stifle the technology — it is to use it, and use it wisely. We must stay a step ahead of illicit actors by leveraging the same innovations they use for bad, for good.

At TRM Labs, we embed AI at every layer of our blockchain intelligence platform to help fight financial crime. We use machine learning models and behavioral analytics to flag complex obfuscation techniques, trace illicit cryptocurrency transactions in real time, and discover novel criminal typologies before they can scale.

In practical terms, this means our tools are continuously becoming smarter and faster. For example, TRM's Signatures® recognizes on-chain patterns linked to known scam campaigns, money-laundering networks, and darknet market activity. And our interactive Graph Visualizer allows investigators to quickly follow digital money trails through hundreds of wallet hops, automatically highlighting and summarizing complex paths of funds a human analyst might struggle to unravel.

Today, TRM is developing and deploying AI "defense agents" at scale to map illicit networks, triage threats, and surface early warning signs to help global law enforcement agencies move faster, trace complex laundering schemes, and focus on the highest-risk activity. These are not theoretical ideas — they are operational tools currently being used in the field that help detect and dismantle illicit networks in real time, often stopping criminal schemes before they can do even more harm.

TRM Labs has actively partnered with law enforcement agencies around the world, providing advanced analytics and investigative leads that have directly contributed to arrests, indictments, and the recovery of victim funds. Through a combination of blockchain tracing, AI-driven pattern recognition, and human expertise, we've assisted in cases ranging from deepfake investment scams and romance fraud to illicit cryptocurrency exchanges laundering ransomware proceeds.

As threat actors scale up their schemes with AI, our collective defenses must scale up as well. It is crucial that law enforcement, financial institutions, and intelligence providers be equipped with cutting-edge investigative technology — and that they work in concert across jurisdictions and sectors to combat these threats. In parallel, we must continue to educate and alert the public about these new dangers. AI will undoubtedly shape the next generation of financial crime, but with collaboration and innovation, it can also become the key to preventing and defeating those crimes.

Guiding Principles for Safe and Effective AI in Law Enforcement

As we consider how to responsibly deploy AI in law enforcement and national security contexts, it's important to emphasize the foundational principles that must govern its use. At TRM Labs, we have learned firsthand that AI must not only be powerful but principled. We recommend the following design principles as a baseline for any AI used in investigative or intelligence settings:

- Guardrails: AI should be explicitly limited to predefined, auditable tasks. These systems must be designed with constraints that prevent unauthorized or unintended behavior.
- Compliance: AI must operate within the legal authorities of each agency and jurisdiction to ensure legal, targeted usage.
- Human Control: Human analysts remain in the loop for critical decisions, with AI initially focused on automating low-risk or repetitive tasks. As trust and oversight mechanisms

mature, selective autonomy could be introduced where mission-appropriate and policy-aligned.

- Transparency: Every action taken by an AI system should be fully traceable. Analysts must be able to understand how a result was generated, and audit logs should enable reproducibility for use in court.
- Flexibility: Law enforcement should not be locked into a single model or vendor. Modular architectures allow agencies to swap in best-in-class models for specific tasks, ensuring long-term adaptability.

These principles are not hypothetical. They reflect what we are already building into TRM's AI-driven tools to ensure they are safe, transparent, and effective for frontline investigators. If adversaries are using AI at scale, we cannot meet this moment with manual processes alone. We must respond with purpose-built AI—anchored in principles that protect both effectiveness and civil liberties.

Policy recommendations: Meeting the AI-enabled crime threat with urgency and coordination

The rapid rise of AI-enabled crime presents a national and global challenge that demands an equally swift and coordinated response.

The Department of the Treasury, alongside law enforcement partners at the FBI, HSI, IRS-CI, and the Department of Justice, as well as regulatory and intelligence agencies across the interagency, must invest in next-generation tools, update outdated legal frameworks, and build new mechanisms for information sharing.

Recommendation 1: Strengthen AI capabilities for financial crime detection and disruption

Congress should fund and prioritize the development and deployment of AI-powered tools for detecting and disrupting crime and national security threats. This includes machine learning models that surface behavioral anomalies, detect deepfake-enabled fraud, trace synthetic identities, and flag laundering typologies across the cryptocurrency ecosystem. These tools must be auditable, secure, and deployable across case management systems at IRS-CI, FinCEN, OFAC, FBI, DEA, USSS, HSI, as well at the defense and national security agencies.

Recommendation 2: Build real-time public-private alerting frameworks

Congress should encourage the development of real-time alerting systems that enable law enforcement, financial intelligence units, and vetted investigative partners to flag suspicious wallet addresses and, through the use of AI agents, notify participating exchanges, stablecoin issuers, financial institutions and other participants. These alerts can trigger temporary administrative holds — pending judicial process — to prevent illicit assets from being quickly moved or laundered. Bad actors, with the help of AI, are moving more quickly than ever, and so must we.

A real-time, AI-enabled alerting framework built on public-private coordination would allow all actors to respond faster, trace smarter, and disrupt more effectively.

Recommendation 3: Modernize legal frameworks to address synthetic crime

Congress should close statutory gaps to address AI-generated threats, including:

- Explicitly criminalizing deepfake impersonation fraud
- Defining and prohibiting synthetic CSAM (child sexual abuse material)
- Modernizing evidentiary standards for AI-altered media

These actions are essential to ensure prosecutors and investigators have the legal tools to pursue AI-driven crimes with the same intensity as traditional fraud, abuse, and exploitation.

Recommendation 4: Equip law enforcement with AI-enabled investigative infrastructure

Agencies at every level must have access to modern investigative capabilities, including blockchain analytics platforms with integrated AI, media authentication tools, and other AI-enabled investigative tools. Congress should allocate dedicated funding for these tools, along with specialized training programs in AI-enabled crime, forensic preservation, disruption techniques, network analysis and prosecutorial readiness.

This investment is not only about technology — but about building capacity in agents, officers, and analysts who must now navigate an increasingly complex threat landscape.

Recommendation 5: Promote public-private collaboration to counter AI threats

No single agency or company can address AI-enabled crime in isolation. TRM Labs partners with law enforcement globally, and victim reports through Chainabuse help surface new scam techniques in real time. These initiatives should be supported, formalized, and scaled through structured public-private partnerships that include technology companies, financial institutions, and community watchdogs.

These are the early warning systems of the AI era. Congress should ensure they are resourced, coordinated, and connected to national enforcement priorities.

AI is a vital tool on the side of good

Artificial intelligence is not inherently good or evil; it is a tool. In the hands of criminals, we have seen how it can enable harm at unprecedented speed and scale. But in the hands of law enforcement, innovators, and vigilant citizens, that same technology can be a powerful force for protection. Today's adversaries are moving fast to leverage AI's potential for exploitation. We must move faster.

Every day at TRM Labs, we witness both the dangers and the solutions inherent in AI technology. We see deepfake scams robbing families of their savings, grooming operations that leave victims devastated, and ransomware crews targeting hospitals and schools with AI-enhanced malware. But we also see how cutting-edge analytics, cross-sector collaboration, and an informed public can turn the tide.

Congress has a critical role to play in shaping a future where AI strengthens — rather than undermines — our financial system, our institutions, and our trust in one another. By updating laws, investing in law enforcement and technology, fostering public-private teamwork, coordinating internationally, and educating the public, we can ensure that the tools of safety evolve as fast as the tools of harm.

TRM Labs is proud to support this mission, and we look forward to continuing our work with the Subcommittee toward these goals.

Thank you again for your time and attention. I welcome your questions.

Mr. BIGGS. Thank you so much. I appreciate all of you and your testimony and very, very interesting. I hope we can get to some deep substance on it today.

I now recognize the gentleman from North Carolina, Mr. Knott, for five minutes.

Mr. KNOTT. Thank you, Mr. Chair.

To the witnesses, thank you for coming to testify today. This is sort of a novel topic, but as each of you have stated clearly, this is a very important topic and development around the blockchain technology, AI technology, it is something that it is only going to become more prevalent and more dominant in just about every area of our life. That is true here in America; that is true overseas. It is going to be one of those paramount moments that is going to be formative. Where were you before? Where were you after?

To that end, as a former prosecutor myself, when I was prosecuting, I came on at the very end of the AI-free crime. I started to see how blockchain and cryptocurrencies and artificial intelligence was infiltrating every area of the criminal world.

To that end, Mr. Redbord, as the use of AI and blockchain technology becomes more common and it becomes more integrated in every avenue, there is obviously access from domestic actors that are criminal and international actors. There is really no border that is recognized. How does that impact the criminal infrastructure as it were when you look at domestic versus international crime and that relationship?

Mr. REDBORD. Thank you so much for the question. Yes, I feel like you would uniquely understand this as a former AUSA as well. We both prosecuted cases in a world where there were networks of shell companies and hawalas in high-value art and real eState used to launder funds. Today, as criminal actors are looking to blockchains and cryptocurrencies we can trace every transaction on an open public ledger, right? There's no more bulk cash smuggling. There's TRM to track and trace the flow of funds.

I think what we see right now is this really interesting convergence between AI crime, as we're going to discuss today, and crypto. Really primarily crypto is often the means of value transfer in these different crimes, right? You see these deepfake scams where they are scams trying to get cryptocurrency from investors or users. They are ransomware actors who are supercharging attacks where cryptocurrency is the payment.

The significant difference now as we're investigating crimes as prosecutors and law enforcement is that we can trace and track every one of those payments on open public ledgers which allow us to do financial crime investigation, really, better than we've ever done it before.

Mr. KNOTT. Is there the ability as you see it to pinpoint with specificity criminal activity and, I would say more importantly, going back to the trust that we need in law enforcement, pinpointing criminal actors? Because it is such a foggy space for many people. Can you pinpoint the actual criminal as opposed to just criminal activity?

Mr. REDBORD. It's a great question, and absolutely in many circumstances. What we're doing essentially at TRM is we're taking that raw blockchain data, right, those alphanumeric addresses,

those crypto wallets, and we're associating them with real world entities. Oftentimes it's terrorist financiers, ransomware actors, and sanctions, for example. That allows law enforcement to then take that data and track and trace the flow of funds to build out networks.

Mr. KNOTT. Is there—

Mr. REDBORD. Cartels are a great example of that today. I'm sorry.

Mr. KNOTT. Is there a risk that cartels, terrorist states could use legitimate constructs on the blockchain that are developed here in the United States for their own benefit, therefore taking advantage of a legitimate structure or a legitimate software that is developed here?

Mr. REDBORD. Absolutely. The real challenge for regulators and policymakers is how to ensure that lawful users have access to those types of tools and yet stop bad actors from using them. To me the answer the U.S. Treasury Department over the last few years has done a pretty good job on this—target the bad actors: The North Korean cyber criminals, the ransomware actors, and the scammers, as opposed to necessarily the lawful services that they're using.

Mr. KNOTT. Is there a risk if we are too zealous in the prosecution? As a prosecutor I am all for strong law enforcement, but if we are too aggressive on the front end as this technology is developing, could we stifle domestic innovation here at home if we are too aggressive in prosecuting?

Mr. REDBORD. Absolutely. It is critical that we continue to focus on the bad actors in this space which will allow the lawful ecosystem to grow as opposed to the lawful services that are being used by bad actors. Absolutely, really the key to all of this is to stop bad actors from leveraging the technology to allow this industry and this technology to grow.

Mr. KNOTT. Then briefly, what can we do in Congress to ensure that law enforcement has the resources to target the bad actors with specificity?

Mr. REDBORD. That's exactly right. Today what we really have across the U.S. Government is a cadre of law enforcement agents that are really true experts, power users of blockchain intelligence tools. What we really need is that cadre to grow significantly. As bad actors are leveraging AI, as they're leveraging blockchain technology, every Federal agent should have access to tools and the training necessary to sort of meet this new moment from a technology perspective.

Mr. KNOTT. Sir, thank you.

Mr. REDBORD. Thank you.

Mr. KNOTT. Other Members, I ran out of time, Mr. Chair. I yield back.

Mr. BIGGS. Thank you. Without objection, I propose that we have a second round of questions. Seeing none, we will proceed in that fashion.

Now, I recognize the Ranking Member, Ms. McBath.

Ms. MCBATH. Thank you, Mr. Chair. I just have to say that—and just in listening to each and every one of the witnesses, I am just really amazed at the depth of the use, criminal usage of AI. Really

thank you so much for what you brought to the table today, but I do want to talk a little bit about facial recognition.

The Detroit Police Department reportedly conducted 129 facial recognition searches in 2020, and all on African American people. The following year 95.6 percent of the searches targeted Black people.

Mr. Venzke, how does the use of AI-enabled facial recognition comply with the Fourth Amendment's equal protection principles?

Mr. VENZKE. It raises serious concerns. As far as I know there's not been a clear holding that equal protection principles are violated by the use of facial recognition technology, but it certainly raises those concerns because of the disproportionate impact we've seen that technology have on protected classes, particularly as you said, Black people, and in particular Black men.

We've also engaged in civil rights litigation to defend individuals who have been wrongly identified by facial recognition technology. To a large extent this is a matter of process, ensuring that police departments have appropriate processes in place so that there isn't reliance solely on an identification made by facial recognition technology to bring in a suspect that there isn't bias in lineups and things of that nature.

Because of the certain threats that we've seen here and the ways that the technology can struggle in real world conditions we have long stood by that there needs to be a moratorium for law enforcement uses of facial recognition Thank you.

Ms. MCBATH. Thank you for that. This is just so interesting you should say that because even on my phone I have facial recognition and sometimes it says I don't recognize you and I am like, well, you know who I am. Of course, there are still problems with AI and the technology still needs to be advanced.

Mr. Venzke, I am going to ask you another question: What warrant requirements and limitations should be applied for facial recognition tools when they are used by law enforcement?

Mr. VENZKE. Well, as I said, our overall stance is that law enforcement should not be deploying the technology at all because of the underlying foundational issues of how it can struggle with a variety of protected classes and correctly identifying people, especially in real world conditions where lighting may not be ideal or the surveillance footage may be grainy. That can result in someone who's 8 months pregnant being apprehended for a crime where there clearly was not a pregnant person involved.

The use of facial recognition technology may not necessarily implicate the Fourth Amendment, but as I said, it raises very serious concerns about perpetual surveillance, the ability of the Federal Government to identify individuals in public spaces going about their daily lives without any recourse, without any judicial oversight. That is ultimately a policy question for legislators, city councils, and Congress to step up and regulate.

Ms. MCBATH. Thank you for that. Dr. Bowne, in your experience have you find that AI-enabled tools used by law enforcement are tested and evaluated before they are deployed to ensure that they are safe and effective?

Dr. BOWNE. In my experience in law enforcement, as a prosecutor, recently as a supervising prosector the tools that are being

used are certainly going to depend on the jurisdiction that's using them. States, counties, certainly Federal Government, from my experience in the Department of the Air Force, law enforcement organizations that are starting to use these tools are relatively new users.

In the Air Force any AI tool is supposed to go through rigorous testing and evaluation standards to ensure that it results in a certain quantified reliability. That's very challenging to do with some of these tools, particularly when you're talking about edge cases like African American men when they are not found frequently in data sets. Those questions are being asked.

I don't see in my experience the type of rigorous standards established across the board by regulators. Until that happens law enforcement is going to try to keep up. It's tempting to do that, but there's likely to be some gaps there.

Ms. MCBATH. Thank you.

Mr. BIGGS. Thank you. The gentlelady yields. I now recognize the gentlelady from Florida, Ms. Lee, for five minutes.

Ms. LEE. Thank you, Mr. Chair.

Welcome to our witnesses today. As a Member of the House's Bipartisan Task Force on Artificial Intelligence I had the opportunity to work with Members on both sides of the aisle to discuss a national approach to artificial intelligence that would encourage innovation, strengthen our global leadership, and also confront serious threats including those like you have been discussing here today that involve criminal misuse of this technology.

Today's hearing, among other things, highlights one of the most urgent of those threats, which is the exploitation of children through AI, from synthetic child abuse materials to predatory chatbots, to real time location spoofing, we are seeing criminals use AI to expand both the scale and sophistication of their crimes. AI can also, we know, be part of the solution. In cases like Operation Renewed Hope AI helped Federal agents identify and rescue minor victims who might otherwise have never been found.

One of the things that we are interested in doing is ensuring that law enforcement, child protection, nonprofits, and trusted partners in the private sector have access to effective responsible AI tools and the legal clarity to use them. It is about stopping criminals, saving lives, protecting children, and ensuring that we are doing our part to help technology be a force for good.

On that subject, Ms. Perumal, I would like to followup with you. I would like to know what would you recommend Congress prioritize, to better equip law enforcement with the tools they need to stay ahead of AI-enabled threats?

Ms. PERUMAL. Thank you so much for the question. I think a few things come to mind. One is strengthening public and private partnerships. The more that we have the opportunity to share information across industry and government, and the threats we're seeing, it is incredibly helpful.

Making it easier to share technology and share the innovation—frankly, it can sometimes be difficult, especially as small business are trying to figure out how to share that technology, which makes a delay. As you have a new way that we can maybe find something like trafficking or better detect AI-generated harm, it can be dif-

ficult to then deploy that. I think anything that is to improve that public-private partnership would be incredibly helpful.

Ms. LEE. Are there specific legislative or funding priorities that you or your clients have identified that you think would be impactful?

Ms. PERUMAL. Yes, few things that we see with our clients. One is there's a big challenge to identity in terms of online identity. The AI-generated agents can more explicitly scrape, use websites for fraud. Then on the other side you also see things like ID fraud where people are using this to hide their identity and commit online crimes.

That's an area that the industry is generally trying to adapt and respond to because that's how so much of fraud and scams and extortion has been carried out.

Another thing that comes to mind is to the earlier point on innovation, if it's easier to share and collaborate, that would be incredibly helpful for us in the private sector.

Ms. LEE. I would like to go back to you, Mr. Redbord. You said something in your remarks that I thought was really interesting, that AI is also the future of enforcement. I believe your words were invest, collaborate, and we can be more effective.

I would like to hear in your view what are the most urgent risks posed by AI to national security and public safety and what would you like to add about what we can be doing in Congress?

Mr. REDBORD. Absolutely. Thank you for the question. Really what we see AI doing today is supercharging criminal activity that we've seen exist for some time. Now, you don't need ransomware affiliates because you can have AI agents that are automatically deploying malware. We're seeing cyber-attacks at scale by Norther Korea and other types of cyber actors. Then we're seeing the laundering of the funds that are stolen move faster than ever before.

As I mentioned in my testimony we've seen a 456-percent increase from last year in scam activity involving AI. We have to move as fast as the criminals. When we think about these issues at TRM, it's how can we move faster? How can we us AI the same way they're moving funds to track and trace those funds to ultimately seize them back?

It's—when you ask, it's the tools and the training to ensure that every single law enforcement and national security professional have access to the same tools that many cyber criminals are using today, and obviously the funding necessary to support that as well as the training.

Ms. LEE. Thank you. Mr. Chair, I yield back.

Mr. BIGGS. The gentlelady yields back. I recognize myself for five minutes. I appreciate the testimony that we have had.

I had a different line of questions for the next round, but things you have said in your testimony and what I have heard in the first round makes me want to ask some specific areas.

You don't have a lot of time to respond, so I am going to ask because I want a quick response from every one of you.

One of you mentioned the ELVIS Act in Tennessee, which prohibits the simulation of Elvis' voice, basically. That is how that generated. What about any other person? I am thinking what if there is a deepfake of any other public figure and you have that

person say something that is pernicious, something that is bad, something that is politically inflammatory, whatever, do we have laws in place that would prohibit that or it's just the Wild, Wild West?

We will start with you, Mr. Redbord.

Mr. REDBORD. Slightly more broadly, I would say that we have laws in place that absolutely cover a lot of these areas, but we are going to need to add AI to a lot of them. When I think about these issues, for example, when you talk about these types of scam activity that are being supercharged by AI, we have wire fraud statutes to address them.

Mr. BIGGS. Right, right. We will get into that, too, but I am talking specific. This is a specific case. Let's say you have a public figure and you have them say something that is totally outrageous, it is totally deepfaked. You can't tell. The average person can't tell. If that person was—if that language is attributed to that person elsewhere, you might have libel. You might have civil claim of libel or defamation of character, something like that. Does that in your opinion exist when someone manipulates a deepfake to do something like that?

Mr. REDBORD. It would require adding additive measures to what we have today.

Mr. BIGGS. Mr. Venzke?

Mr. VENZKE. That sort of speech lies at the core of the First Amendment's protections. It's a commentary on politicians. For example, when the—

Mr. BIGGS. If it is not commentary on politicians. Let's say with maliciousness. Maliciousness? With malice. That is the word I am looking for. With malice you say that Andy Biggs said X, Y, this. It is just horrible. You put it in <it>The New York Times and you did it because you wanted to harm me.

Mr. VENZKE. If you take, for example, the Republican National Committee's deepfake about President Biden announcing a draft for Ukraine, that is commentary on public events. Of course, existing exceptions to the First Amendment still apply to AI. That means—

Mr. BIGGS. That is what I want to get at. That is what I wanted to hear from you, whether something like a defamation, like—

Mr. VENZKE. Yes, defamation is subject to—

Mr. BIGGS. —which is why I specifically used <it>*The New York Times*.

Mr. VENZKE. That's exactly right.

Mr. BIGGS. Ms. Perumal, same question?

Ms. PERUMAL. Yes, I am not super familiar with the legal side, so I can talk more the technology, but I do see that it is challenging, detection on it.

Mr. BIGGS. Right. Thanks. Dr. Bowne?

Dr. BOWNE. There's this inherent friction that we see. I agree with both Mr. Redbord and Mr. Venzke, that what you described, sir, is likely protected under the First Amendment. You have—

Mr. BIGGS. Unless there is malice.

Dr. BOWNE. With malice. Now, there's legal protection certainly from a civil right of action if it were to be—

Mr. BIGGS. Let's not to interrupt. I don't want to be rude to interrupt, but I do want to interrupt. What my question is—let's expand it. A true deepfake is so persuasive you can't tell the difference side-by-side of me over here and the deepfake. We have had examples of parents and grandparents. They can't tell the difference between the deepfake and the voice of the kid. They look the same. They act the same. They are remarkable. Now, do I have protection, for instance, from someone doing that?

This is going to lead into the CSAM, which I was hoping I would have enough time to get to that, because it is the same type of deal where you see CSAM, which is so persuasive and sick and disgusting. That is all AI-generated. You mentioned the one of the Ukraine thing. What remedy does someone have when they are a victim of this kind of generative AI?

Dr. BOWNE. Mr. Chair, if it were to fall under the statute of like wire fraud—so you look at the intent of what's behind it. Those are protections there. If it's to create misinformation, you certainly articulated the challenge and the potential harm, that may not be outside of the law. There are gaps in protection when you're facilitating particularly harmful activity using deepfakes.

Mr. BIGGS. Yes, thank you. We will be talking about that in the future.

That ends the first round of questioning and now for the second round of questioning I recognize the gentleman from North Carolina, Mr. Knott.

Mr. KNOTT. Thank you, Mr. Chair. I have got to say I am happy to have a second round so soon. I wished more Members would show up because this is important, but selfishly I am enjoying the conversation.

All of you have basically indicated what was stated either directly or indirectly that computational power and ability will dictate sort of the new criminal landscape. Obviously, AI will supercharge this. The landscape is going to be forever changed. I want to ask each of you, how far are we from having autonomous criminal behavior?

Doctor, start with you. Go in order down the line.

Dr. BOWNE. Those are fantastic questions.

Mr. KNOTT. Thank you.

Dr. BOWNE. My assessment is we're there. We have plenty of autonomously certainly, from a bad actor that is using AI and using the autonomous features of those models to perpetuate crimes we're certainly there. The scale, the sophistication, and the speed that are created by using AI-enabled models, certainly, from committing scams at scale, targeting personally, finding cyber vulnerabilities, that is all happening already.

Ms. PERUMAL. Yes, I agree. We're definitely seeing that now. It's the beginning of what's happening. It's being used for more simple crimes. We see different uses. You might think of simple bots that text people and send us these annoying scam text messages. Those are using AI and automate by pulling breached or leaked data about you. Then, similarly with computer-use agents, they're starting to be filling out forms. There's a large opportunity for those to get much more sophisticated.

Mr. VENZKE. Relatedly on the civil side, we're seeing rapid advancement of artificial intelligence that's used to make decisions about who can get a loan, who has access to house, and things of that nature. Often in many cases that will output a score that humans are largely deferring to. Artificial intelligence has reached the point where it is having an outsized effect on our lives, not just because of criminal activity, but because it affects so many important sectors as well.

Mr. KNOTT. Yes.

Mr. REDBORD. Thank you for the question. We are there today, but AI is not dominating criminal activity. That's in large part why this hearing is so important at this moment, to start having this conversation. This is really why at TRM over the last year or so we have focused a lot of our attention. Particularly how can we build AI tools that enable us to move faster? Because while we're not there yet, we're getting very, very close.

Mr. KNOTT. What is going to be required to make it responsive to the threat?

Mr. REDBORD. That's exactly right.

Mr. KNOTT. What will be required? I am asking, like—

Mr. REDBORD. Oh, sorry.

Mr. KNOTT. —in terms of capacity, in terms of private sector investment, in terms of public investment? Give me a broad picture of what's going to be needed.

Mr. REDBORD. It's all of it. I know public-private partnerships were talked about. It's often this sort of this right way as something to discuss. Really what it has to be is the private sector building the tools that government can ultimately leverage to move as fast as the cyber criminals.

Mr. KNOTT. In your opinion is the law lagging this new frontier or are the existing criminal laws sufficient to protect the marketplace and victims like Mr. Biggs talked about?

Mr. REDBORD. It'll absolutely be a combination of both. It will be important when you talk about CSAM, which I know we'll focus on, on ensuring that the Federal sentencing guidelines meet the AI moment for that. We will have a need for AI-specific laws, but I will say that a lot of the laws we have today: Wire fraud, bank fraud, those types of laws, these types of disinformation investigations, certainly will include AI.

Mr. KNOTT. Jurisdictionally how do you see AI factoring into content actions, vehicles designed overseas that penetrate into the American market? How do we protect against that in a jurisprudence sense?

Mr. REDBORD. It's a challenge. The nature of crypto, the nature of AI, and the nature of technology, is global and cross-border. In large part we want to make sure that the innovation is happening here. That's why it's so important that as we have these conversations we're walking that line between stopping bad actors but not stifling innovation in this critical moment. Just like the internet was born and created in the United States we need to ensure that is true for AI technology as well.

Mr. VENZKE. If I may add to that representative, as we think about ways that existing legal frameworks need to adapt to this rapidly evolving challenge, a multijurisdictional approach is the

right approach, not just at the Federal level, but also internationally, and of course with States. We've talked a little bit about the moratorium that was included in versions of the reconciliation package. The House did exempt criminal laws. Often, in many cases, civil penalties will be a necessary complement, for example, in addressing nonconsensual imagery at high schools—

Mr. KNOTT. One more question for the panel really quick. What can parents do to protect their children from this type of landscape?

Dr. BOWNE. As a parent myself, education on the risk is certainly important. That's something that the public sector can lead on, law enforcement can lead on, similar to drugs and tobacco. The risk of AI, whether it's for scams, whether it's for CSAM, whatever harms, they really impact children as well.

Ms. PERUMAL. I definitely agree. Especially for the CSAM harms, giving their children awareness that something like this might happen to you, it might have nothing to do with anything you did and here's how you can reach out. Sharing that awareness because they target the fact that people feel shame when they have no reason to. I think that would be really helpful.

Mr. KNOTT. Thank you.

Mr. VENZKE. As a former teacher parents are an integral part in helping kids navigate the world, and education and talking with kids about the new risks that are emerging are critical.

Mr. KNOTT. Thank you.

Mr. REDBORD. Education is absolutely critical. As a parent of middle school and high school-aged kids I appreciate this. One more point that I do think is important here though is that we need to ensure that they also know how to leverage it, not that they're just afraid of it.

Mr. KNOTT. Sure.

Mr. REDBORD. Their success in large part and in the rest of their life will depend on their ability to leverage and engage with this technology. It's absolutely so critical that on the one hand we protect them against the bad harms, but also ensure that they're really able to use it and leverage it.

Mr. KNOTT. Absolutely. Thank you. Mr. Chair, I yield back.

Mr. BIGGS. Thank you. The gentleman yields. We now recognize now the Ranking Member, Ms. McBath.

Ms. MCBATH. Thank you, Mr. Chair. Once again, as you can see, we are quite alarmed as to what we are hearing today, so thank you very much.

I want to go back and touch on what the Chair was just asking, the question that he asked about. In specific, I would just—each of you, if you can just tell us in a nutshell that you are expressing to us that there are gaps. There are gaps in legislation. There are gaps in things that we need to do here in Congress to make sure that there are protections that are enforcing and preventing these kinds of deepfakes and all that we are talking about today.

Can you give us an idea? Tell us what kinds of legislation are going to be extremely important for us to put in place to prevent these kinds of gaps that you just expressed to us that there are today?

Dr. Bowne, could you start, please?

Dr. BOWNE. Yes, ma'am. One of the gaps may be closed soon. H.R. 1283, which was introduced by this Committee would amend Title 18 of the U.S.C. 2252(a), which is the statute that covers child pornography and CSAM. The bill is intended to amend that statute to include AI-generated CSAM within the definition and coverage under that criminal statute. There is the Title 18, the criminal statutes that may need to be amended both in content on what is covered, what is criminalized, but also potentially in the sentencing guidelines, as Mr. Redbord mentioned.

Then, as the Chair explained and in his question there is a gap as well on the civil side that there might not be a cause of action for that noncriminal, because even that amendment that's proposed in H.R. 1283 still has to be constitutional. There are First Amendment protections even on things that would normally be objectionable.

Ms. MCBATH. OK. Thank you. Mr. Redbord, please?

Mr. REDBORD. Thank you very much. I provided about five suggestions in my written testimony, but I'll just focus on one for purposes of this answer.

It is absolutely critical that agencies at every level have access to modern investigative capabilities including the blockchain analytics platforms integrated with AI, media authentication tools, as we talked about, and AI-enabled investigative tools. Congress should allocate dedicated funding to these tools along with specialized training programs.

Ms. MCBATH. Thank you. Mr. Venzke?

Mr. VENZKE. I think awareness of, first, where existing law can apply to criminal activity is critical in navigating this space. For example, 2258(a) has been extended and prosecutions have been brought for simulated CSAM material created regarding a specific identifiable child using AI technology. I agree with Mr. Redbord that education, providing training, defense, and funding for critical infrastructure for schools and others to educate students and other vulnerable populations about the threats of AI will be key, and to shore up their own cybersecurity infrastructure.

Ms. MCBATH. Mr. Venzke, I want to go back to something that you did touch on though. You did touch on the moratorium on State and local AI, which actually failed. That last attempt failed. The Republican Chair of the House Energy and Commerce Committee has already vowed to continue to pursue it even as they acknowledge that Federal legislation setting standards on AI is still years away.

As we work to develop that legislation what principles or proposals should we consider?

Mr. VENZKE. One thing I would look to, and Representative Lee already referenced it, was the House AI Task Force final report from the last Congress. That was a thoughtful sort of compendium of the various issues around AI regulation at the Federal level. It recognized that preemption particularly is a sensitive issue. It doesn't need to be all or nothing, that there is a range of tools that can be used in adjusting what is the appropriate area for preemption? What is the program amount of preemption to ensure that States have significant latitude to address these harms in a timely

manner, which of course is beneficial for Congress as this Committee looks at what works and what does not.

Ms. MCBATH. OK. Thank you. One last question. Dr. Bowne, how can public agencies use the procurement process to ensure that the AI systems they want to acquire are safe and effective?

Dr. BOWNE. They certainly articulate what the problem is and what the need to create a demand signal for private industries, for R&D, for academia to do the research that is needed. The procurement system is a fantastic way for Federal agencies or State agencies to ensure that the standards are being met and that the capabilities are there and are being focused on in the development and the research in the public sector—or in the private sector and in academia.

Ms. MCBATH. Thank you. Mr. Chair, I have a unanimous consent request to enter into the record, a statement from Barry Friedman, Faculty Director of the Policing Project at New York University School of Law, dated July 16, 2025. Also, entering into the record a statement for record dated July 16, 2025, from Public Citizen regarding the growing threat of criminal exploitation through AI. Last, but not least, a unanimous consent to enter into the record a statement from Keith Kupferschmid, Chief Executive Officer of the Copyright Alliance, dated June 13, 2025.

[The information referred to follows:]

Mr. BIGGS. Without objection.

Ms. MCBATH. Thank you. I yield.

Mr. BIGGS. Thank you. The Chair now recognizes the gentleman from California, Mr. Kiley, for his five minutes.

Mr. KILEY. Thank you, Mr. Chair, for calling this hearing. It is a hugely important topic. We have often seen this arms race develop between criminals and law enforcement when it comes to the use of technology where criminals innovate and law enforcement has to innovate in turn. It is a matter of just trying to sort of keep up.

With AI it is a totally different ball game in the sense that the development of new capabilities is happening so quickly, and the nature of those capabilities is often emergent and surprises even the people who train the systems. The ways in which they are being applied is equally unpredictable.

To me it seems that integrating AI into law enforcement operations, is not just a tool at this point; it is absolutely essential. It is a tremendous challenge and requires a lot of expertise. It seems to me that we need to be thinking very seriously about how we can have coordination and how we can make cutting-edge tools available to law enforcement across the country.

I wanted to ask both Mr. Redbord and Ms. Perumal, if I am saying that correctly, about your thoughts on this. I know that you have a law enforcement background. I know that you actually worked at Google, and I believe it was just a couple days ago that Google announced that its cybersecurity AI platform for the first time detected and defeated a software vulnerability in the wild that was known to malevolent actors. Maybe if you could both address the role of the public and private sector in meeting this challenge.

Mr. REDBORD. Thank you so much for the question. It's absolutely critical that the public and private sector work together on this as the question noted.

Look, every Federal law enforcement agency in the U.S. today is using tools like TRM to track and trace the flow of funds, to automate tracing when it comes to cryptocurrency, to leverage AI tools in that respect. The reality is that it's still a handful of investigators that have this expertise and training.

As we move from crime on city streets to crime on blockchains and in cyberspace we're going to need every agent and investigator, not just Federal, but State and local to have access to these types of tools and training. As you mentioned, cyber criminals are now using this more and more and will eventually be using this at scale. Every agent investigator who is investigating these cases, tracking them, needs to be moving as quickly. I would say tools and training primarily.

Then the other piece is really true public-private partnership where FBI and IRS-CI and HSI and others are working closely with the private sector to share information to move as quickly as possible.

Mr. KILEY. Thanks very much.

Ms. PERUMAL. Thank you for the question. I love that you're following the vulnerability discovery. That's awesome.

To your point the criminal ecosystem is using this to scale their offense. We have to use it to scale our defense and make that more effective if we're going to keep up. There's a lot of ways we can do that, from better detecting malware, to better understanding the tools and tactics they're using, better detecting the scam messages. If we can enable, as I said, the public-private partnerships, which we keep repeating and if we can make it easier and much faster to adapt as the criminal ecosystems adapts, that makes us a lot more effective.

There are so many opportunities. Even if you think about all the reports of scams that maybe we already have access to or law enforcement has access to, if we can just go through that data and find the trends, using AI to speed up and scale investigations is a way that we can really keep pace with the criminal ecosystem.

Mr. REDBORD. One more thing I would add to that, historically, I was a prosecutor for a long time, we investigate specific cases, right? There's an instance of crime and we need to investigate that specific case. What this technology really allows us to do is build out networks, to understand crime typologies, to understand where the threat actors are, and how they are engaging and what they would potentially do next. Really, it's an extraordinary moment when it comes to not just law enforcement, but how to disrupt adversaries from a national security perspective.

What this technology—and I think you got to this in your question—really enables is not just the one-off harm that's been done to an individual, but how do we build out networks of cartels, fentanyl dealers, and scam networks in Southeast Asia and elsewhere? This technology I guess connected to blockchain intelligence, really allows us to do a lot of that today.

Mr. KILEY. Interesting. You can address crime much more systematically in a more efficient way and more preemptively?

Mr. REDBORD. We even see that today in the actions that are coming from the U.S. Treasury and Department of Justice where they're going after networks. They're doing civil forfeitures. There was a very large civil forfeiture complaint filed about 2 weeks by the U.S. Attorney's Office in D.C., against $225 million involved in pig butchering scams. It was a network. We're seeing them use it today.

Mr. KILEY. Very interesting. Thanks very much. Mr. Chair, it seems there is a role perhaps for us to play in supporting these public-private partnerships and in facilitating the training and access to this knowledge and these resources in law enforcement across the country. I yield back.

Mr. BIGGS. Thank you. The gentleman yields back. I am going to recognize myself for my last five minutes here. I would suggest that as we started off, I said this would be the first of its kind. I meant that we are going to have to keep pushing this.

A week—let's see, maybe a week ago Elon Musk announced Grok 4. He talked about artificial intelligence and Grok 4 is going to have the intelligence—it already has beyond a Ph.D., engineering, science, genius, et cetera, an artificial super intelligence.

We've touched on it lightly here today using different terms, but my question is at what point do we no longer see computational decisionmaking with a human first mover and you have an algorithmically iterative process that essentially—and we are there in some extent now, but we are not totally there because human interaction is still the first mover. At some point it won't be a human that is the first mover anymore; it will be the algorithm itself.

How long before we get there? How do we get there and prevent the crime and provide the deterrence that is necessary? For the hypothetical I give you, how long before adjudicating whether there is probable cause or not for a search warrant or an arrest warrant is merely algorithmically sustained as opposed to having a human make that determination?

With that bizarre question but acknowledging that we are actually moving so rapidly that we probably thought by 2050 you would be getting to artificial super intelligence, but it looks like maybe before 2030 you are going to be in artificial super intelligence.

Dr. Bowne? Then we will go down the whole panel.

Dr. BOWNE. Thank you, Mr. Chair. Certainly, a thought-provoking exercise. I am glad we are still at the point where it is an exercise, and not reality, but I recognize that we may not be far from there.

Before we get to artificial general intelligence, or before we get to certainly artificial super intelligence—and those are still theoretical and not a foregone conclusion—there is this very powerful and very rapidly increasing agentic AI.

Mr. BIGGS. Yes.

Dr. BOWNE. We start to see some of what you describe already taking place at, admittedly, lesser extent than what we would if it were true AGI or ASI. We still have algorithms that are making decisions on behalf of humans that are able to do so at speed and often at a skill that it certainly makes it difficult for the human agent to observe and to be a part of. It really depends on how much

trust, how much authority we provide those agents, and what those models are; they fine-tuned to limit that?

I do believe, as you said, Mr. Chair, this is the first of hopefully many having some of those industries, some of those private sector companies describe that so that this Subcommittee and Congress can ensure that they are able to predict and know, and set up those guard rails if necessary to limit what you're concerned about.

Mr. BIGGS. Ms. Perumal? Since we only have a minute left, each of you get 20 seconds.

Ms. PERUMAL. Thank you. Very interesting question. We see AI agents making simple decisions today. For more complex decisions, as the models can do more complex reasoning in the next few years, it really should come down to how important is the decision, and then what transparency and explainability we can get from the model and how much human oversight is necessary? It really depends on how risky that individual decision is where we should hopefully see it overlap on these autonomous decisions.

Mr. VENZKE. I'm going to build directly on that. The role of AI is a choice. Laws passed in Texas, the National Security Memorandum that governs national security uses AI, say that certain things are off limits for artificial intelligence.

You mentioned probable cause. That strikes me as a core foundational tenet of due process that should probably be truly a human activity. That is the choice that we make of who will be—what will be human, what will be AI, and where will humans be in the loop?

Mr. REDBORD. I've never seen anything move as fast as this moved in my lifetime. While I don't have a great answer for how long, it's certainly coming. If I could leave this Committee with anything today, it's that we need to move as quickly building the tools, working with this body to provide the right laws there. As an old school prosecutor, I'm happy with judges still making decisions around probable cause, but I do think we really need to ensure that we are using the tools defensively to meet this moment.

Mr. BIGGS. Great. Thank you all for being here. My time is expired. There is so much more to cover about this. Like I say it is just the first, and hopefully we will get back together soon and continue this.

Please feel free to contact me or the Ranking Member. I assume that is OK. She says that is OK. Because we want to have a dialog and see where there are holes, where there are gaps. Let us know. We want to do stuff that is preventive without being constrained, if that is possible. Thank you.

With that, we are adjourned.

[Whereupon, at 11:30 a.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Crime and Federal Government Surveillance can be found at: *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118467*.

○