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.