epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA
+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

House Committee on Energy and Commerce
Subcommittee on Communications & Technology
2125 Rayburn House Office Building
Washington, DC 20515-6115

Hon. Robert E. Latta and Hon. Doris Matsui,
Thank you for the opportunity to testify before the Subcommittee on Communications and Technology on January 11, 2024, as part of your hearing "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era." As I discussed in my testimony, the security of communications has implications not only for privacy generally but also specifically for national security, public safety, and trust in the marketplace. Please find below EPIC's responses to the additional questions submitted by Hon. Lizzie Fletcher and Hon. Debbie Dingell.

--

Hon. Lizzie Fletcher,
Thank you for your additional questions about artificial intelligence (AI) and cybersecurity, including cybercrime and cybersecurity strategies specific to open-source models.

Fundamental principles in AI development, such as ensuring security, privacy, fairness, transparency, and accountability, apply regardless of whether the AI system is based on open source or closed source software. Both types of AI systems are susceptible to adversarial attacks, where malicious actors manipulate inputs to exploit AI algorithms.[1] These include poisoning attacks, evasion attacks, and model inversion attacks.[2] Robust training, randomized smoothing, and formal verification mechanisms can help detect and mitigate these adversarial inputs.[3] Both types of AI systems, like any piece of software, may also be subject to unaddressed vulnerabilities generally.[4]

Any model that relies upon open source components may also be vulnerable to library-based attacks. These includes lookalikes (mimicking the name of authentic packages) as well as injecting malicious code into authentic packages.[5]

AI systems, in particular, are also vulnerable to data leaks, inferences, and harmful secondary uses. Possible solutions include use of synthetic data and utilizing quasi-open models rather than wholly open-source models. There are numerous examples of data leaks from AI-powered products, including

[1] *See* Vassilev A, et al., Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, NIST Artificial Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2023 (Jan. 2024), https://doi.org/10.6028/NIST.AI.100-2e2023.
[2] *See id.*
[3] *See id.*
[4] *See id.*; *see also* Stan Kaminsky, Open source: the top-10 risks for business (Apr. 13, 2023), https://www.kaspersky.com/blog/open-source-top-10-risks/47875/ (using outdated versions of components can exacerbate this problem).
[5] *See* Kaminsky (noting that up to 80% of code within open-source projects is derived from other sources in the form of dependencies).

both leaks of PII to users and leaks of user conversations to third parties.[6] Data inferences and combined datasets can produce information that is just as sensitive as PII used in training—or even input data itself—especially where government datasets are combined with commercial datasets. Synthetic data may be a viable method for guarding against adversarial attacks designed to obtain this information.[7]

In terms of harmful secondary uses, especially in the context of open-source models, AI-powered tools can be repurposed for malicious ends.[8] One possible solution here may be to opt instead for quasi-open models—for example, allowing users to adjust model weights without giving users access to the full model.

Two additional concerns with open source AI models are jailbreaking systems and market concentration. If applying guardrails to an open source model, it may be easier for a bad actor to strip away the guardrails ("jailbreak" the model) and deploy a version of the model that doesn't include those guardrails (especially if those guardrails were not included in the initial release of the product). Market concentration can also implicate cybersecurity concerns, as compromising such a widespread system can result in catastrophic-level failures.[9]

Many AI risks are fundamentally rooted in the data used to train AI systems, making data security a crucial foundation for addressing these risks. Vulnerabilities in data security can enable malicious hackers to exploit AI models, accessing private information or manipulating outputs for harmful purposes. Regulations upon collecting, processing, auditing, and utilizing AI training data is an essential first step, such as advancing the principle of data minimization, under which only essential data is collected and utilized.[10]

We again thank you for your interest in this issue and would be happy to discuss concerns about AI, privacy, and cybersecurity with you further.

--

[6] *See, e.g.*, Bill Touulas, OpenAI rolls out imperfect fix for ChatGPT data leak flaw, Bleeping Computer (Dec. 21, 2023), https://www.bleepingcomputer.com/news/security/openai-rolls-out-imperfect-fix-for-chatgpt-data-leak-flaw/; Ram Shankar Siva Kumar, A Few Useful Lessons about AI Red Teaming, HAI Seminar (Oct. 18, 2023), https://hai.stanford.edu/events/ram-shankar-siva-kumar-few-useful-lessons-about-ai-red-teaming.

[7] *See* Christian Reimsbach-Kounatze et al., *Emerging Privacy Enhancing Technologies: Current Regulatory & Policy Approaches*, 351 OECD Digit. Econ. Papers 4 (Mar. 2023), https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm.

[8] *See* Rhiannon Williams, Text-to-image AI models can be tricked into generating disturbing images, MIT Technology Review (Nov. 17, 2023), https://www.technologyreview.com/2023/11/17/1083593/text-to-image-ai-models-can-be-tricked-into-generating-disturbing-images/.

[9] *See, e.g.*, Bruce Schneier, Click Here to Kill Everybody (2018).

[10] *See* Comments of EPIC to NIST, Request for Information Related to NIST's Assignments Under Sections 4.1, 4.5, and 11 of the Executive Order Concerning Artificial Intelligence, No. 2023-28232 (Feb. 2, 2024), available at https://epic.org/epic-urges-nist-to-center-ai-transparency-and-data-minimization-in-ai-risk-management-following-biden-executive-order/.

Hon. Debbie Dingell,
Thank you for your inquiry about third party access to consumer vehicular data, including safety risks resulting from potential cybersecurity vulnerabilities.

Connected vehicles with advanced sensors and wireless communication technologies, such as Bluetooth, Wi-Fi, or cellular networks, are able to exchange data in real-time between vehicles, infrastructure, and external services. Third-party access to consumer vehicular data by automakers, app developers, service providers, data brokers,[11] and others poses significant privacy and security risks. This consumer data may encompass sensitive information such as vehicle location, driving behavior, vehicle health, and personal preferences. For example, a recent report from Mozilla exposed the broad range of personal information that cars might collect about us (including medical information, genetic information, sexual activities, speed at which one drives, locations visited, and media played).[12] The Mozilla report found that the majority (84%) of the automotive companies reserve the right to sell and share personal information, and in the vast majority of cases (92%) drivers are not given control over their data.[13]

Car manufacturers could put measures in place to better protect the data generated or collected by their vehicles, but have largely opted not to. The Alliance for Automotive Innovation created a list of privacy-preserving principles such as "data minimization" and "transparency" that many car brands signed on to.[14] Despite signing on, however, car brands do not seem to follow these principles.[15]

Beyond privacy-based concerns, there are also vehicle safety-related concerns. Tesla's AI-powered autopilot was reportedly involved in 17 deaths and 736 crashes and is currently the subject of multiple government investigations.[16] This occurred without any evidence of malicious interference, and there is evidence to suggest that vehicles may be susceptible to remote hacking.[17]

---

[11] This can have frightening implications for personal safety. *See, e.g.*, FCC Chairwoman Calls on Carmakers and Wireless Companies to Help Ensure the Independence and Safety of Domestic Violence Survivors (Jan. 11, 2024), https://www.fcc.gov/document/chairwoman-safe-connected-cars-domestic-violence-survivors.
[12] *See* Jen Caltrider, et al., It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy, Mozilla Privacy Not Included (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ [hereinafter "Mozilla Report"]; *see also* M. Hadi Amini, Your car might be watching you to keep you safe – at the expense of your privacy, The Conversation (Dec. 6, 2023), https://theconversation.com/your-car-might-be-watching-you-to-keep-you-safe-at-the-expense-of-your-privacy-213213.
[13] Mozilla Report.
[14] *See* Alliance for Automotive Innovation, Inc., Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services (last reviewed March 2022), https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_Vehicle Technologies_Services-03-21-19.pdf.
[15] *See* Mozilla Report.
[16] *See id.*
[17] *See, e.g.*, Ionut Arghire, Researchers Hack Remote Keyless System of Honda Vehicles, Security Week (Mar. 28, 2022), https://www.securityweek.com/researchers-hack-remote-keyless-system-honda-vehicles/ ; Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway-With Me in It, Wired (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

We again thank you for your interest in this issue and would be happy to discuss concerns about connected devices (including cars), location data, and personal and public safety with you further.

Respectfully,

Alan Butler
/s/ Alan Butler
Executive Director and President
Electronic Privacy Information Center (EPIC)
1519 New Hampshire Avenue NW
Washington, DC 20036