

The Honorable Todd Blanche
Attorney General of the United States
U.S. Department of Justice

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives

The Honorable Chuck Grassley
Chairman
Committee on the Judiciary
United States Senate

The Honorable Ted Cruz
Chairman
Committee on Commerce, Science, and
Transportation
United States Senate

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Jamie Raskin
Ranking Member
Committee on the Judiciary
U.S. House of Representatives

The Honorable Dick Durbin
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and
Transportation
United States Senate

The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives

September 30, 2026

Dear Attorney General Blanche, Chairman Jordan, Chairman Grassley, Chairman Cruz, Chairman Guthrie, Ranking Member Raskin, Ranking Member Durbin, Ranking Member Cantwell, and Ranking Member Pallone:

We, the undersigned organizations, write to urge the Department of Justice and Congress to immediately investigate the growing number of cybersecurity and safety incidents involving AI agents developed and deployed by OpenAI, Anthropic, Google, Meta, and other leading artificial intelligence companies. Reporting indicates the number of security incidents being investigated by leading AI companies is [in the tens of thousands](#) which represents an unprecedented violation of our digital infrastructure.

For several months, these companies have collectively and repeatedly demonstrated that the risks posed by advanced AI models are no longer hypothetical: their systems have hacked private companies, gained unauthorized access to government systems, compromised sensitive information, and caused real-world harms. Measures taken by these companies to oversee AI development and secure against these threats have proven inadequate. AI companies have also acknowledged their failure to detect cyber security incidents until days or weeks after they occurred. These stunning admissions underscore the recklessness by which these companies are pursuing AI products. The companies acknowledge they cannot safely research their own technology during testing nor reliably account for their products upon introduction to the marketplace. Companies that choose to develop autonomous AI systems, or any product for that matter, must assume responsibility for harms caused by their products. Big Tech cannot race to deploy AI and treat automation or their collective inability to monitor, control, and account for AI systems as an excuse to avoid liability.

The following are just a sampling of the growing number of security incidents involving agentic AI products that have come to light:

- OpenAI failed to prevent its models from gaining [unauthorized access to an Australian government healthcare system](#) and accessing non-public files prompting an [investigation](#).
- OpenAI failed to prevent its models gaining unauthorized access to the [U.S. Department of Commerce and Census Bureau systems](#).
- OpenAI failed to prevent its agents from unauthorized activity involving SEC.gov and Investor.gov and subsequently [posting the information elsewhere](#).
- Anthropic failed to prevent Claude models from [compromising four separate organizations](#).

- Anthropic has [documented](#) repeated instances in which malicious actors circumvented its safeguards and used Claude in cyber operations, surveillance, fraud and other harmful activities. Anthropic's own threat reporting demonstrates that safeguards imposed by frontier AI companies [remain vulnerable](#).
- Meta confirmed that its safeguards failed resulting in a model [breaching an external company's system](#) during third-party testing.
- Shortly after Meta launched its AI agent, Muse, a researcher discovered a vulnerability that could [allow an attacker to take control of a user's account and access personal files](#).
- During cybersecurity evaluations, Google's safeguards failed to prevent Gemini models from accessing the open internet and [gaining unauthorized access to systems belonging to three real companies](#).
- OpenAI failed to prevent its AI agents from [exploiting vulnerabilities in Hugging Face](#), executing code across dozens of servers, obtaining root-level access, and accessing private information and credentials. OpenAI's agents copied private evaluation data into a publicly accessible dataset, demonstrating the company's inability to prevent its product from exposing third-party data. OpenAI later acknowledged that employees had [observed warning signs weeks earlier](#), exposing failures in the company's internal processes for identifying, escalating, and responding to harmful outcomes.
- OpenAI recently confirmed that its agents publicly [posted 53 images belonging to ChatGPT users without authorization](#).

AI companies cannot escape accountability simply by attributing this conduct to their AI products. Companies in other industries routinely deploy products capable of acting with varying degrees of automation. A self-driving taxi company cannot blame the vehicle when its technology injures a passenger. Airlines cannot disclaim responsibility for unsafe automated flight systems that result in crashes upon take-off and landing. A bank cannot evade civil rights laws by blaming an algorithm for discriminatory lending decisions. **The same basic principle must apply to artificial intelligence.**

Existing law already provides mechanisms for addressing unauthorized access to computer systems, including the [Computer Fraud and Abuse Act](#). Whether these incidents violated that law or other statutes is ultimately a question for independent investigators and, where appropriate, the courts. But more than two months after the OpenAI-Hugging Face incident became public, the first of such public disclosures, there has been no public congressional hearing examining these events and no publicly-announced Department of Justice investigation. That response is difficult to reconcile with the seriousness with which the United States treats unauthorized intrusions into government and private computer systems when they are attributed to foreign adversaries, criminal hacking organizations, or individuals.

We therefore urge:

1. **The Department of Justice to immediately open an investigation** into these incidents and determine whether federal laws were violated; and
2. **Congress to immediately convene public oversight hearings**, compel production of relevant records where necessary, and require testimony under oath from executives and other relevant parties.

At a moment when Americans [across the political spectrum are demanding greater oversight and accountability for artificial intelligence](#), the federal government is woefully absent. It is clear that Congress must enact stronger safeguards to reduce AI risks before harms occur. In the meantime, Congress and the Trump administration have an immediate duty to enforce existing law and hold companies accountable for harms caused by the AI systems they develop and deploy.

Sincerely,

Public Citizen
Americans for Responsible
Innovation
Tech Oversight Project
All Girls Allowed, Inc.
BESC
Black Voters Matter Fund
Concerned Health
Professionals of
Pennsylvania
Consumer Action
Consumer Federation of
America
Common Cause
Demand Progress
Education Fund
Enabled Emissions
Campaign
Future of Life Institute
Green Peace USA
Greisinger Family Tree
Farm
Guardrails Action
Income Movement

Indivisible
Interfaith Center on
Corporate Responsibility
Investor Alliance for
Human Rights
Irreplaceable
Issue One
La Fontaine Residents
MARBE SA
Marcus on AI, Gary
Marcus
Mothers Against Media
Addiction (West Los
Angeles)
Move Past Plastic (MPP)
MPower Change Action
Fund
National Coalition Against
Cryptomining
NAVA (National
Association of Voice
Actors)
NETWORK Lobby for
Catholic Social Justice

Novadaur
Oil and Gas Action
Network
Oregon Consumer Justice
People Power United
Physicians for Social
Responsibility
Pennsylvania
Preserving Hollenback
Roots
Stand.earth
The Alliance for Secure AI
The Human Line Project
Three Rivers Waterkeeper
Too many to list
Voices for Progress
Who Decides
Women's International
League for Peace and
Freedom US
Young People's Alliance
350 Yakima Climate
Action