THE COLLABORATION ON ADVERSARIAL THREATS AND SECURITY RISKS ACT

The Threat: Foreign adversaries, including China, are running deliberate, industrial-scale campaigns to steal America's most advanced AI models through illegitimate "distillation" attacks: bombarding a U.S. model with prompts to clone its capabilities at a fraction of the cost. These attacks expose vulnerabilities across developers.

- Anthropic caught Chinese labs using roughly 24,000 fraudulent accounts to harvest more than 16 million exchanges from its models; OpenAI and Google have released similar reports.
- The White House has accused China of conducting "deliberate, industrial-scale campaigns to distill U.S. frontier AI systems."
- As AI models become more capable, experts warn these attacks will allow foreign models to pose national security and public safety risks.

The Problem: Developers identify these attacks first, but legal uncertainty around coordinating responses with competitors discourages collaboration on threat assessments, testing, or safeguards. Current law permits ***cyber*** *threat-sharing*, but no equivalent protection exists for ***AI*** *threat-sharing*.

The Solution: The Collaboration on Adversarial Threats and Security Risks Act creates a targeted affirmative defense to allow AI developers to collaborate in good faith exclusively to address a covered AI-security risk. The bill includes strict safeguards to prevent an overly broad application, while ensuring U.S. developers are able to counter foreign espionage and the most serious AI security risks.

HOW THE BILL WORKS

What Companies Can Do	What Stays Illegal
Share threat information and assistance specific to covered AI security risks, such as theft, distillation, weaponization, etc. of American models by adversaries.	Price-fixing, market allocation, boycotts, and monopolization. Companies bear the burden of proof, must give DOJ advance written notice before any coordinated action, and are liable for any violation of antitrust laws or coordination on actions outside of covered AI security risks, as well as any bad-faith conduct.

BIPARTISAN, BICAMERAL, AND BROADLY BACKED

Led by Rep. Bob Latta (R-OH) and Rep. George Whitesides (D-CA) in the House and Sen. Adam Schiff (D-CA) and Sen. Jim Banks (R-IN) in the Senate.

Supporting Organizations: Software Information Industry Association (SIIA), Google, Encode AI, Association for Competitive Technology (ACT), Health Information Sharing and Analysis Center (Health-ISAC), Law Reform Institute, SeedAI, AI Policy Network (AIPN), and others.

Questions: Dahvi Cohen (Dahvi_Cohen@schiff.senate.gov), Charlie Mlcek (charlie.mlcek@mail.house.gov)