

US and allies tighten AI oversight amid cyberattacks and legal tests

Executive Summary

The past few days saw a step towards global coordination on AI oversight while new risks emerged. The Trump administration approved sharing advanced AI models with the UK's safety institute (www.usnews.com [1]), reversing a prior ban and signalling a cooperative stance. Meanwhile, a surge of AI-enhanced cyberattacks in Asia (www.insurancejournal.com [2]) and a US lawsuit over AI-driven pricing (money.usnews.com [3]) are underscoring the urgent need for businesses to strengthen their AI governance and risk management practices.

References:

- [1] [www.usnews.com](https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=developers%20%E2%80%8Bcan%20give%20the%20British,with%20Britain%27s%20AI%20Security%20Institute) — <https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=developers%20%E2%80%8Bcan%20give%20the%20British,with%20Britain%27s%20AI%20Security%20Institute>
- [2] [www.insurancejournal.com](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=Newsletter%20Article%20%20Comments%20South,is%20helping%20attackers%20automate%20tasks) — <https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=Newsletter%20Article%20%20Comments%20South,is%20helping%20attackers%20automate%20tasks>
- [3] [money.usnews.com](https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions#:~:text=hyperlink%20in%20paragraph%205,it%20says%20restaurant%20%E2%80%8BCowners%20should) — <https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions#:~:text=hyperlink%20in%20paragraph%205,it%20says%20restaurant%20%E2%80%8BCowners%20should>

US allows model-sharing for UK AI safety tests

In a significant policy shift, the United States is now permitting its artificial intelligence companies to share their most advanced models with the United Kingdom's AI safety authorities. A Reuters report revealed that the Trump administration has reversed an earlier decision that had discouraged developers like OpenAI and Anthropic from providing the UK's AI Safety Institute with early access to new AI models (www.usnews.com [1]) (www.usnews.com [2]). The UK established its AI Safety Institute after a 2023 global summit to evaluate high-risk AI systems for dangerous behaviour (www.usnews.com [3]). By lifting restrictions on cross-border model sharing, the White House is signalling a more collaborative approach to managing AI risks internationally.

This U-turn by Washington marks a departure from the previous stance that treated advanced AI models as a national asset to be guarded. The change comes as regulators worldwide press for greater transparency and cooperation on AI governance. Europe's landmark AI Act - the world's first comprehensive AI law, which began taking effect in August (www.trust.org [4]) - is already influencing companies beyond the EU's borders (www.trust.org [5]). The newly open US-UK pipeline for model testing suggests that even under a pro-industry administration, governments recognise that complex AI challenges like "rogue" AI agents and safety assurance can't be solved in isolation. For businesses developing cutting-edge AI, this means they should prepare for more engagement with regulators and potentially sharing information about high-impact systems for safety validation. Global convergence on AI standards may simplify compliance in the long run, but it also raises the bar: organisations must ensure their AI governance and risk controls meet the stricter expectations emerging across jurisdictions.

References:

- [1] [www.usnews.com — https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=developers%20E2%80%8Bcan%20give%20the%20British,with%20Britain%27s%20AI%20Security%20Institute](https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=developers%20E2%80%8Bcan%20give%20the%20British,with%20Britain%27s%20AI%20Security%20Institute)
- [2] [www.usnews.com — https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=administration%2C%20the%20Telegraph%20newspaper%20said,Spokespersons%20for](https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=administration%2C%20the%20Telegraph%20newspaper%20said,Spokespersons%20for)
- [3] [www.usnews.com — https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=developers%20greater%20latitude%20to%20cooperate,advanced%20AI%20models%20to%20evaluate](https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says#:~:text=developers%20greater%20latitude%20to%20cooperate,advanced%20AI%20models%20to%20evaluate)
- [4] [www.trust.org — https://www.trust.org/2026/07/28/new-report-reveals-extent-eu-ai-act-influence/#:~:text=Global%20Impact%20of%20The%20EU,research%20indicates%20that%20companies%20that](https://www.trust.org/2026/07/28/new-report-reveals-extent-eu-ai-act-influence/#:~:text=Global%20Impact%20of%20The%20EU,research%20indicates%20that%20companies%20that)
- [5] [www.trust.org — https://www.trust.org/2026/07/28/new-report-reveals-extent-eu-ai-act-influence/#:~:text=long,key%20trends%20down%20for%20investors](https://www.trust.org/2026/07/28/new-report-reveals-extent-eu-ai-act-influence/#:~:text=long,key%20trends%20down%20for%20investors)

South Korea and Japan act on AI-driven cyberattacks

Authorities in Asia are responding to a new wave of cyberattacks powered by AI. In September, Japanese companies including a major bank, a telecom firm and a retail chain suffered 86 AI-assisted cyber incidents - an 18% jump from the previous month (www.insurancejournal.com [1]). In South Korea, nine banks and other organisations were also targeted by hackers using tools like AI agents to automate hacking tasks from finding software vulnerabilities to writing phishing emails (www.insurancejournal.com [2]) (www.insurancejournal.com [3]). According to government data, South Korea saw 1,236 cyber incidents in the first half of 2026, a 20% increase over the prior year (www.insurancejournal.com [4]). Security experts warn that artificial intelligence is lowering the technical bar for criminals and enabling faster, stealthier attacks (www.insurancejournal.com [5]) (www.insurancejournal.com [6]).

Financial and technology regulators in both countries have ordered swift action. South Korea's Financial Services Commission directed banks and other financial firms to complete a 12-point cybersecurity self-assessment in light of the breaches (www.insurancejournal.com [7]). In Tokyo, Japan's digital minister convened emergency meetings, and the National Cybersecurity Office is issuing new warnings to businesses (www.insurancejournal.com [8]). Although recent attacks have not yet caused major losses, analysts at Fitch warn that victims could face regulatory penalties, customer compensation and higher cyber security costs if AI-driven breaches continue (www.insurancejournal.com [9]). For corporate leaders, the message is clear: as AI becomes a tool for attackers, companies must include AI-specific threat scenarios in their risk assessments and strengthen security governance accordingly. Ensuring robust oversight of any AI systems in use - especially those handling sensitive data or critical operations - can help meet rising regulatory expectations and mitigate the growing cyber risks.

References:

- [1] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=view%20is%20that%20Japan%20is,South%20Korean%20bank%20incidents%20would](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=view%20is%20that%20Japan%20is,South%20Korean%20bank%20incidents%20would)
- [2] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=been%20hit%20by%20a%20recent,the%20year%20than%20in%20all](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=been%20hit%20by%20a%20recent,the%20year%20than%20in%20all)
- [3] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=cybersecurity%20specialists%20say%20the%20technology,The%20rise%20suggests%20attackers%20have](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=cybersecurity%20specialists%20say%20the%20technology,The%20rise%20suggests%20attackers%20have)
- [4] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=them%2C%20E2%80%9D%20he%20said,The%20South%20Korean%20bank](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=them%2C%20E2%80%9D%20he%20said,The%20South%20Korean%20bank)
- [5] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=been%20hit%20by%20a%20recent,the%20year%20than%20in%20all](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=been%20hit%20by%20a%20recent,the%20year%20than%20in%20all)
- [6] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=has%20largely%20erased%20language%20and,powered%20tools%20are%20also](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=has%20largely%20erased%20language%20and,powered%20tools%20are%20also)
- [7] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=AI%20in%20some%20capacity%20and,%20E2%80%9CThe%20attackers%20have](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=AI%20in%20some%20capacity%20and,%20E2%80%9CThe%20attackers%20have)
- [8] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=AI%20in%20some%20capacity%20and,%20E2%80%9CThe%20attackers%20have](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=AI%20in%20some%20capacity%20and,%20E2%80%9CThe%20attackers%20have)
- [9] [www.insurancejournal.com — https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=testing%20as%20AI%20evolves%2C%20Meyers,about%20AI%20E2%80%99s%20growing%20role%20in](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm#:~:text=testing%20as%20AI%20evolves%2C%20Meyers,about%20AI%20E2%80%99s%20growing%20role%20in)

McDonald's AI pricing sparks antitrust challenge

McDonald's is confronting a novel legal threat over its use of artificial intelligence in setting menu prices. A class-action lawsuit filed in a US federal court on 2 October alleges that the fast-food giant's AI-driven pricing tool effectively pushed its 14,000 franchise restaurants into price-fixing (money.usnews.com [1]). According to the complaint, McDonald's requires franchisees to use a centralised "pricing engine" that adjusts menu prices using an algorithm, which the plaintiffs claim has resulted in coordinated higher prices for products like Big Macs and fries across otherwise independent outlets (money.usnews.com [2]). The case is part of a broader trend: similar lawsuits have accused companies in hospitality, real estate, and insurance of using algorithms to collude on prices and harm consumers (money.usnews.com [3]). McDonald's has denied the allegations, telling Reuters that its franchise owners set prices individually and that "AI does not set the price of a Big Mac or any other menu item" (money.usnews.com [4]).

This lawsuit raises pressing questions about how existing laws apply to AI-enabled business strategies. Antitrust regulators and courts are being forced to consider whether algorithmic pricing tools might inadvertently violate competition laws (money.usnews.com [5]). For companies, it's a warning that adopting AI for key decisions - especially those affecting markets or customers - should involve rigorous legal and ethical oversight from the outset. Compliance chiefs are already bracing for a tide of new AI-related regulations (kpmg.com [6]), and this case suggests enforcement of traditional laws like antitrust will also extend to AI-driven practices. Businesses should review any AI systems that coordinate pricing, marketing, or other competitive strategies to ensure they have proper governance checks in place and do not facilitate unintended collusion.

References:

- [1] money.usnews.com — <https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions#:~:text=Plaintiffs%20have%20sued%20companies%20in,McDonald%E2%80%99s%20told%20Reuters%20%E2%81%A0that>
- [2] money.usnews.com — <https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions#:~:text=action%20lawsuits%20around%20the%20country%2C,McDonald%E2%80%99s%20told%20Reuters%20%E2%81%A0that>
- [3] money.usnews.com — <https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions#:~:text=hyperlink%20in%20paragraph%205,in%20which%20most%20of%20%E2%80%8Cits>
- [4] money.usnews.com — <https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions#:~:text=14%2C000%20US%20restaurants%20are%20independently,lawsuit%20followed%20%E2%80%8Ba%20Reuters%20report>
- [5] money.usnews.com — <https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions#:~:text=nickel,nothing%20inherently%20illegal%20about%20using>
- [6] kpmg.com — <https://kpmg.com/xx/en/our-insights/risk-and-regulation/2026-kpmg-global-cco-survey.html#:~:text=priority%2075,AI%20use%2C%20having%20seen%20more>

Tesla rebrands 'Full Self-Driving' after safety scrutiny

In Europe, regulators have compelled Tesla to change how it markets its automated driving technology. The company has dropped the name "Full Self-Driving (Supervised)" - often known as FSD - and now calls the option "Assisted Driving" in its European markets (www.cnbc.com [1]). German authorities took issue with the "Full Self-Driving" label, deeming it misleading since the system still requires an attentive human driver and is not truly autonomous (www.cnbc.com [2]). (In the United States, Tesla continues to use the old branding and charges a \$99 monthly subscription for the feature (www.cnbc.com [3]).) The forced rebranding underscores how consumer protection and safety regulators are increasingly cracking down on exaggerated or ambiguous claims about AI capabilities.

The move by German regulators reflects a wider push for transparency and accountability in AI products. Under forthcoming EU rules and standards, companies will be expected to provide clear information about AI-driven features - from labelling AI-generated content to clarifying the limits of automation in critical functions. If even a leading tech company like Tesla must adjust its product marketing to stay on the right side of the law, other businesses should take note. For any AI system that interacts with customers or impacts safety, businesses need to ensure their product descriptions, user communications, and risk disclosures are accurate and compliant. Building these considerations into product governance from the start can prevent regulatory run-ins and safeguard consumer trust.

References:

- [1] [www.cnn.com — https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html#:~:text=Tesla%20has%20changed%20the%20brand,99%20per%20month%20subscription%20for](https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html#:~:text=Tesla%20has%20changed%20the%20brand,99%20per%20month%20subscription%20for)
- [2] [www.cnn.com — https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html#:~:text=Tesla%20has%20changed%20the%20brand,99%20per%20month%20subscription%20for](https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html#:~:text=Tesla%20has%20changed%20the%20brand,99%20per%20month%20subscription%20for)
- [3] [www.cnn.com — https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html#:~:text=Tesla%20has%20changed%20the%20brand,99%20per%20month%20subscription%20for](https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html#:~:text=Tesla%20has%20changed%20the%20brand,99%20per%20month%20subscription%20for)

Key Statistics

- 36% of CFOs confident they can drive AI impact (Gartner, 2025)
- 33% of compliance officers citing new regulations as top challenge (KPMG, 2026)
- 12.4% of companies worldwide have a human oversight policy for AI (Thomson Reuters Foundation, 2026)
- 1,236 cyber incidents in South Korea in H1 2026, up 20% year-on-year (S. Korea government data, via Reuters)
- 50% of UK CFOs expecting AI-driven productivity gains in next 12 months (Deloitte, 2026)

KEY TAKEAWAY

Identify where your business uses AI in high-stakes areas like pricing, safety or customer data, and tighten oversight. Involve legal, compliance and security teams early - proper governance can prevent costly incidents and speed safe innovation

Sources

- [US Reverses Course on Britain's Testing of AI Models, Telegraph Says](https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says)
<https://www.usnews.com/news/top-news/articles/2026-10-11/us-reverses-course-on-britains-testing-of-ai-models-telegraph-says>
- [South Korea, Japan buffeted by hacks as AI lowers bar for cybercriminals](https://www.insurancejournal.com/news/international/2026/10/09/888570.htm)
<https://www.insurancejournal.com/news/international/2026/10/09/888570.htm>
- [AI Pricing Lawsuit Against McDonald's Raises New Antitrust Questions](https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions)
<https://money.usnews.com/investing/news/articles/2026-10-08/analysis-ai-pricing-lawsuit-against-mcdonalds-raises-new-antitrust-questions>
- [Tesla drops 'Full Self-Driving' name in Europe after regulator push](https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html)
<https://www.cnn.com/2026/10/09/tesla-full-self-driving-europe-regulator.html>
- [EU AI Act Drives Global AI Governance Beyond Europe | Study](https://www.trust.org/2026/07/28/new-report-reveals-extent-eu-ai-act-influence/)
<https://www.trust.org/2026/07/28/new-report-reveals-extent-eu-ai-act-influence/>
- [2026 KPMG Global Chief Ethics and Compliance Officer Survey](https://kpmg.com/xx/en/our-insights/risk-and-regulation/2026-kpmg-global-cco-survey.html)
<https://kpmg.com/xx/en/our-insights/risk-and-regulation/2026-kpmg-global-cco-survey.html>
- [Gartner Survey Shows Top Priorities for CFOs in 2026 Include Cost Optimization, Improved Forecasting, and Funding Growth Opportunities](https://www.gartner.com/en/newsroom/press-releases/2025-08-12-gartner-survey-shows-top-priorities-for-cfos-in-2026-include-cost-optimization)
<https://www.gartner.com/en/newsroom/press-releases/2025-08-12-gartner-survey-shows-top-priorities-for-cfos-in-2026-include-cost-optimization>
- [Deloitte CFO Survey Q2 2026: Growing AI optimism](https://www.deloitte.com/uk/en/about/press-room/deloitte-cfo-survey-quater-two-2026-growing-ai-optimism.html)
<https://www.deloitte.com/uk/en/about/press-room/deloitte-cfo-survey-quater-two-2026-growing-ai-optimism.html>

