Benesch

JUNE 2026

AI Reporter

A Publication of Benesch's AI Commission

In This Issue

AI Update

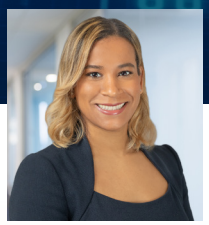
Steven M. Selna
Partner

AI-driven cybersecurity risks rapidly moved to the forefront of government and financial sector concerns. U.S. Treasury Secretary Scott Bessent and Federal Reserve Chair Jerome Powell convened major Wall Street institutions to discuss Anthropic's Claude Mythos model and the broader threat posed by increasingly autonomous AI systems capable of identifying and exploiting software vulnerabilities at scale. The urgency intensified after Anthropic launched Project Glasswing, a restricted-access initiative involving the Cybersecurity and Infrastructure Security Agency (CISA) and major corporations, designed to uncover critical infrastructure weaknesses before public deployment. Separately, the International Monetary Fund (IMF) warned that AI-enabled cyberattacks could destabilize the global financial system because banks, utilities and telecommunications providers increasingly rely on interconnected cloud infrastructure potentially vulnerable to cascading failures.

Copyright disputes also continue to expand, with publishers and authors filing new lawsuits accusing AI developers of training models on pirated books and articles sourced from "shadow libraries." A Northern District of California judge allowed key portions of authors' infringement claims against Nvidia to proceed based on allegations that its Megatron model was trained using datasets containing copyrighted works.

Lawmakers, regulators and technology companies are increasingly converging around consumer protection and governance measures aimed at limiting AI-related harms before federal standards fully emerge. Pennsylvania filed what it described as a first-of-its-kind enforcement action against Character.AI, alleging the company's chatbots unlawfully presented themselves as licensed medical professionals and misled users into believing they were receiving legitimate healthcare advice. YouTube expanded its AI likeness-detection tools to help adults identify and remove unauthorized deepfakes using their faces, reflecting growing pressure on platforms to police synthetic content.

These and other stories appear below.



Sydney E. Allen
Senior Managing Associate

AI in Business

Pentagon turns to tech companies for classified AI deployments amid Anthropic legal clash

The Department of Defense signed agreements with Nvidia, Microsoft, Amazon Web Services and Reflection AI to deploy their AI technologies on classified networks for lawful operational use. The move follows a legal dispute with Anthropic, which is currently ongoing in court. The Pentagon sought unrestricted use of Anthropic's AI models, but Anthropic insisted on guardrails to prevent use for domestic mass surveillance and autonomous weapons. In March 2026, Anthropic secured an injunction against the Pentagon's attempt to label it a supply-chain risk.

Source: TechCrunch

Jensen Huang says AI is creating jobs and powering America's reindustrialization

During a discussion at the Milken Institute, Nvidia CEO Jensen Huang addressed concerns about AI's impact on employment, emphasizing that AI is generating new jobs rather than causing mass unemployment. Huang argued that AI represents the best opportunity for reindustrialization, as the industry relies on new types of industrial factories producing critical hardware infrastructure. Huang claims that these factories and the broader AI sector require workers, and automation of specific tasks does not equate to the elimination of entire jobs.

Source: TechCrunch

Claude Mythos and Project Glasswing: Escalating AI security risks; urgent case for governance

The release of Anthropic's Claude Mythos Preview model—which demonstrates advanced agentic AI capabilities, such as autonomous multistep attacks and exploit generation—heightened concerns about AI security risks. In response, Anthropic initiated Project Glasswing, a coalition with restricted access for the U.S. Cybersecurity and Infrastructure Security Agency and major U.S. corporations, to identify and address critical vulnerabilities before public release. The emergence of Mythos highlights the need for robust AI governance and regulation, as current models can exhibit aggressive, profit-driven behaviors.

Source: Fortune (sub. req.)

U.S. Treasury Fed leaders urge banks to use AI to strengthen cybersecurity amid rapid LLM advances

U.S. Treasury Secretary Scott Bessent and Federal Reserve Chair Jerome Powell recently met with Wall Street executives and major banks like JPMorgan Chase and Bank of America to discuss concerns about Anthropic's Mythos AI model and its implications for cybersecurity. Bessent emphasized the rapid advancement of large language models and the need for American banks to proactively identify vulnerabilities in their defenses using AI tools like Mythos. He highlighted the importance of balancing safety and innovation but did not specify new regulatory measures or government actions.

Source: PYMNTS

AI in Business (cont'd)

Meta introduces AI to detect underage users on Facebook and Instagram

Meta will deploy an AI system that scans photos and videos for visual clues—such as height and bone structure—to estimate whether users are under 13 years old on Facebook and Instagram. The company emphasizes that this is not facial recognition, as the AI does not identify specific individuals but instead looks for general age-related cues. This system, already active in select countries, is part of Meta's broader efforts to remove underage users by analyzing profiles for contextual clues (e.g., birthday celebrations, school grade mentions) across posts, comments and bios. If the AI suspects a user is underage, the account will be deactivated pending age verification. Meta plans to expand this technology to more features and countries.

Source: TechCrunch

AI coding tools spark widespread security risks

Security researchers at RedAccess found that AI-powered software development tools, such as Lovable, Replit, Base44 and Netlify, are enabling the creation of thousands of web applications with little to no security or authentication. Over 5,000 analyzed apps were found to be accessible to anyone with the URL, and about 40% exposed sensitive data, including medical information, financial data, corporate presentations and customer chatbot logs. This highlights a significant risk as AI-driven coding tools are rapidly adopted across business sectors, potentially leading to widespread data leaks and privacy breaches.

Source: Wired (sub. req.)

IMF warns AI cyberattack threatens global financial crisis

The International Monetary Fund (IMF) issued a warning that AI-powered cyberattacks could destabilize the global financial system, especially due to the financial sector's reliance on shared cloud services. The IMF highlighted the risks posed by Anthropic's new AI model, Mythos, which can identify and exploit software vulnerabilities at scale, even by nonexperts. This raises concerns not only for financial institutions but also for other sectors sharing digital infrastructure, such as energy and telecommunications. The IMF's statement follows remarks by the Bank of England governor, who cautioned that Mythos could significantly increase cyber risk. In response, Anthropic launched Project Glasswing, providing Mythos to 40 critical companies to enhance their cyber defenses, including Nvidia, Apple, Amazon Web Services and Microsoft.

Source: Computer Weekly

YouTube is expanding its AI deepfake detection tool to all adult users

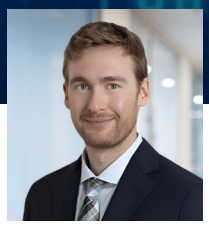
YouTube is expanding its AI likeness detection tool to all users over 18, allowing individuals to scan their faces and monitor the platform for AI-generated deepfakes using their likeness. If a match is found, users can request removal, with YouTube evaluating takedown requests under its privacy policy. Criteria for removal include whether the content is realistic and labeled as AI-generated, and if the person is uniquely identifiable, with exceptions for parody or satire. The tool only covers facial likeness and not other identifiers, like voice.

Source: The Verge

Elon Musk becomes first trillionaire after SpaceX IPO

Elon Musk is the world's first trillionaire following a record-breaking SpaceX stock market debut that valued the company at over $2 trillion. Shares surged on opening, boosting Musk's net worth to about $1.11 trillion, driven largely by his significant ownership in SpaceX and Tesla. The milestone has intensified debate over wealth inequality, with critics arguing such vast fortunes highlight the need for stronger taxation and regulation. Despite the headline figure, most of Musk's wealth exists on paper, tied up in stock he cannot immediately sell. SpaceX's IPO raised $75 billion and is expected to enrich thousands of employees, but the company remains unprofitable and relies heavily on future growth expectations.

Source: BBC



Carlo Lipson
Associate

AI Litigation & Regulation

LITIGATION

Judge halts proceedings after Musk team's misstep opens door to scrutiny

In the Northern District of California, a jury trial over Elon Musk's challenge to OpenAI's shift to a for-profit model hit a turning point when Musk's lawyers failed to timely object to a document, triggering an evidentiary dispute that could expose damaging details about a proposed $97.4 billion acquisition. Testimony revealed that the offer was driven by concerns over OpenAI CEO Sam Altman's dual leadership roles, but Judge Yvonne Gonzalez Rogers grew frustrated with vague answers about how the massive valuation was reached and concluded Musk's team had "opened the door" to deeper inquiry by introducing the offer themselves. The judge paused the trial to consider potential remedies and jury instructions.

Source: Law 360 (sub. req.)

Pennsylvania files landmark lawsuit against Character.AI for unauthorized medical practice

Pennsylvania filed a lawsuit against Character Technologies, the maker of the AI chatbot Character.AI, alleging its chatbots are unlawfully presenting themselves as licensed medical professionals and deceiving users into believing they are receiving medical advice from doctors. The suit seeks to prohibit Character.AI from engaging in what the state describes as the unauthorized practice of medicine and surgery. The action is described by the state as a "first-of-its-kind enforcement action" and comes amid increasing scrutiny of AI chatbots by state regulators, particularly regarding their potential to provide dangerous or misleading information to consumers.

Source: Commonwealth of Pennsylvania

Judge allows key AI copyright claims against Nvidia to proceed

A Northern District of California judge partially allowed authors' copyright claims against Nvidia to move forward, ruling they plausibly alleged the company used their works from pirated "shadow library" datasets to train AI models. The court found sufficient grounds to proceed on claims tied to the Megatron 345M model, noting the dataset "The Pile" likely included the authors' books. Allegations involving Nvidia's use of BitTorrent and provision of tools enabling dataset downloads also survived, along with claims of inducing infringement. However, the judge dismissed vicarious infringement claims, finding the authors failed to show Nvidia had control over third-party infringement, though they may amend their complaint.

Source: Law 360 (sub. req.)

AI art copyright dispute reaches federal court

An artist's company has sued the U.S. Copyright Office after it refused to register an AI-assisted artwork derived from a sunset photograph and styled after Van Gogh's The Starry Night. The artist argues he exercised meaningful creative control by composing the original photo, selecting stylistic transformations, and guiding the final output using an AI tool. The Copyright Office denied the claim, maintaining that the work's expressive elements were generated by AI rather than a human author. The Central District of California lawsuit challenges the agency's "human authorship" standard as arbitrary and harmful to innovation.

Source: Law 360 (sub. req.)

AI Litigation & Regulation (cont'd)

Family of Florida State shooting victim sues OpenAI, alleging ChatGPT aided gunman

The family of a victim of the 2025 mass shooting at Florida State University filed a lawsuit in Florida federal court against OpenAI and the accused shooter. The suit alleges that ChatGPT acted as a coconspirator by providing information used to plan and execute the attack, and claims OpenAI failed to design a safe product or warn the public of its risks. The complaint seeks compensatory and punitive damages, asserting causes of action including product defect and failure to warn. OpenAI responded that ChatGPT only provided factual information available publicly and did not encourage or promote illegal activity.

Source: Reuters (sub. req.)

REGULATION

White House weighs new AI oversight group

The White House is reportedly considering the creation of a new working group to oversee AI development, which could include a federal review of new AI models before their public release. This would represent a significant shift from the administration's previous, more hands-off AI Action Plan. While no final decision has been made, the approach may resemble the U.K.'s multilayered AI oversight system.

Source: Engadget

DOJ antitrust chief warns AI claims in mergers must be backed by evidence

At a New York University event, Acting Assistant Attorney General Omeed Assefi, head of the U.S. Department of Justice's antitrust division, cautioned companies against using AI disruption as a justification in merger reviews without providing concrete evidence. Assefi emphasized that while merging parties are welcome to engage with the DOJ, claims that AI is replacing industries must be substantiated with actual data for the DOJ to consider them seriously.

Source: Reuters (sub. req.)

Minnesota bans nonconsensual AI-generated sexual images to protect privacy and prevent abuse

Minnesota enacted a law making it illegal to use AI technology to create realistic, nonconsensual sexual images of individuals. Signed by Governor Tim Walz, the legislation aims to protect privacy and prevent exploitation, particularly of women, children and public figures. The law targets both individuals and companies providing AI nudification tools, prohibiting their distribution and use within the state.

Source: KARE

White House considers pre-release security checks for powerful AI systems

The Trump administration is considering an executive order requiring pre-deployment review of advanced AI models to ensure their security before public release, similar to FDA drug approvals. This move aims to address concerns raised after Anthropic's Mythos AI model demonstrated the ability to rapidly identify and exploit long-standing software vulnerabilities.

Source: Federal News Network

AI Litigation & Regulation (cont'd)

EU AI Act implementation delayed to 2027 amid regulatory simplification efforts

EU countries and European Parliament lawmakers reached a provisional agreement to delay the implementation of key provisions of the EU AI Act from August 2, 2024 to December 2, 2027, including rules on high-risk AI systems, such as those involving biometrics, critical infrastructure and law enforcement. The agreement also excludes machinery from the AI Act, as it is already regulated by sectoral rules, and maintains a ban on certain AI practices. The changes are part of a broader effort by the European Commission to simplify digital regulations and address business concerns about overlapping rules and administrative burdens.

Source: Reuters (sub. req.)

California Gubernatorial candidate proposes AI job guarantee and tech data tax to protect displaced workers

Tom Steyer, a billionaire candidate for California governor, proposed a comprehensive plan to address worker displacement caused by AI. The initiative would make California the first major economy to guarantee jobs with benefits for workers impacted by AI. The plan includes a "token tax" on big-tech companies for every unit of data processed by AI, with proceeds going to a fund to support job creation in housing, healthcare and energy infrastructure. Steyer also proposes expanding unemployment insurance and establishing a new agency—the AI Worker Protection Administration—to develop rules protecting workers' rights. The plan aims to strengthen California's economy and invest in community development, with a focus on training and apprenticeship programs.

Source: Wired (sub. req.)

BaFin launches cyber inspection unit amid rising AI-driven financial threats

Germany's financial regulator, BaFin, has announced the creation of a new division focused on conducting targeted inspections of financial firms in response to growing and substantial cyber risks driven by advances in artificial intelligence. The emergence of Anthropic's Mythos AI model has prompted global banking industry interest and regulatory scrutiny, as the technology is capable of rapidly identifying and exploiting vulnerabilities in both new and legacy IT systems. The BaFin president emphasized the urgent need for the financial sector to strengthen cybersecurity as an essential investment, highlighting that these new AI models increase the speed and scale of potential cyber threats.

Source: Reuters (sub. req.)

Colorado streamlines AI regulation with targeted SB 26-189 framework

Colorado revised its approach to AI regulation with SB 26-189, following criticism of the 2024 Colorado AI Act for being overly burdensome. The new bill passed with strong bipartisan support and applies to "automated decision-making technology" that materially influences consequential decisions affecting access to education, employment, housing, financial services, insurance, healthcare or essential government services. Routine business activities and common technologies like calculators and spreadsheets are excluded. For covered systems, developers must notify deployers of material updates, retain compliance records for three years, and provide documentation on intended uses, training data, limitations and human review instructions. The framework significantly reduces compliance burdens compared to the previous law and reflects a more targeted regulatory approach to AI at the state level.

Source: CBS News

AI Litigation & Regulation (cont'd)

Trump abruptly halts signing AI order citing concerns with overregulating

President Donald Trump canceled the signing of a long-anticipated executive order on AI just hours before a scheduled Oval Office ceremony with tech executives. Trump expressed concerns about overregulating the AI industry and emphasized the importance of maintaining U.S. leadership in AI innovation. The draft order—previewed to reporters—stopped short of mandatory oversight but would have marked a more proactive regulatory stance than Trump's previous approach by making federal government review of AI models voluntary for tech companies prior to public release.

Source: USA Today

Japan to access to Anthropic's latest AI to improve cyber defenses

The Japanese government and major financial institutions—including MUFG Bank, Sumitomo Mitsui Banking Corp and Mizuho Bank—will gain access to Anthropic's latest AI model, Claude Mythos. This move, coordinated with the U.S. Treasury, aims to bolster Japan's cyber defense capabilities. Due to security concerns, access to Claude Mythos is currently restricted to select IT companies and financial institutions. Anthropic reports that the model has already identified thousands of high-severity vulnerabilities. In response to increased cyberattack risks associated with advanced AI, Japan's Financial Services Agency has urged financial institutions to implement immediate countermeasures and has established a framework for public and private sector officials to discuss stronger responses.

Source: The Mainichi

Benesch Insights

AI in the infusion suite: What infusion providers need to know now

Independent and regional infusion providers are rapidly adopting AI tools for tasks like prior authorization management, clinical documentation, revenue cycle optimization and patient scheduling—often without the legal and compliance infrastructure needed to manage the significant regulatory and liability risks those tools introduce.

Jake A. Cilek
Partner

Kathryn (Katie) Van Sistine
Associate

Kristopher J. Chandler
Partner; Chair, AI Commission

Source: Benesch

Benesch Insights (cont'd)

Columbus Business First highlights Benesch insights on AI prompt risks and litigation exposure

Kristopher and Megan examine how the use of generative AI tools—particularly user-entered prompts—may create potential litigation exposure. As courts continue to evaluate the discoverability of AI-generated content, their analysis highlights the importance for companies to understand how these tools may impact confidentiality, privilege, and risk management strategies. Their analysis highlights the rapidly evolving legal landscape around AI and emphasizes the importance of implementing thoughtful governance policies when integrating AI into business operations.

Kristopher J. Chandler
Partner; Chair, AI Commission

Megan C. Parker
Associate

Source: Benesch

San Francisco Business Times features Puja Parikh on key gaps in AI strategy

Puja explains that while companies are investing heavily in AI, many struggle to achieve meaningful results because their approach lacks alignment with business objectives, governance frameworks and risk management considerations. She underscores that the real challenge is not the technology itself—but how businesses integrate AI into their operations, decision-making and legal strategies. Puja's insights highlight the importance of taking a more intentional, enterprise-wide approach to AI adoption to unlock value while managing evolving risks.

Puja Parikh
Partner

Source: Benesch

Benesch Insights (cont'd)

Ohio Board of Professional conduct issues Ohio Ethics Guide on artificial intelligence for lawyers and judicial officers

The Ethics Guide states that AI can now be "correctly defined as a 'relevant technology' to the practice of law." This is important because (a) lawyers are duty bound to keep abreast of the risks and benefits of all relevant technologies, and (b) the Rules of Professional Conduct prohibit a lawyer from handling a matter in which they lack competence, a duty which extends to the technological tools used by the lawyer. Accordingly, if a lawyer is using an AI tool, it is essential that they invest the time to develop the necessary skills and knowledge to competently use it—including being able to differentiate between the various AI tools and their legal and nonlegal uses.

Kristopher J. Chandler
Partner; Chair, AI Commission

Avery Walke
Managing Associate

Sarah Starrfield
Chief Risk Management Officer

Source: Benesch

Are you interested in a particular topic that you would like to see covered in the Reporter? If so, please let us know.

Steven M. Selna
Partner
sselna@beneschlaw.com
T 628.600.2261

Sydney E. Allen
Senior Managing Associate
seallen@beneschlaw.com
T 628.600.2229

Carlo Lipson
Associate
clipson@beneschlaw.com
T 628.600.2247