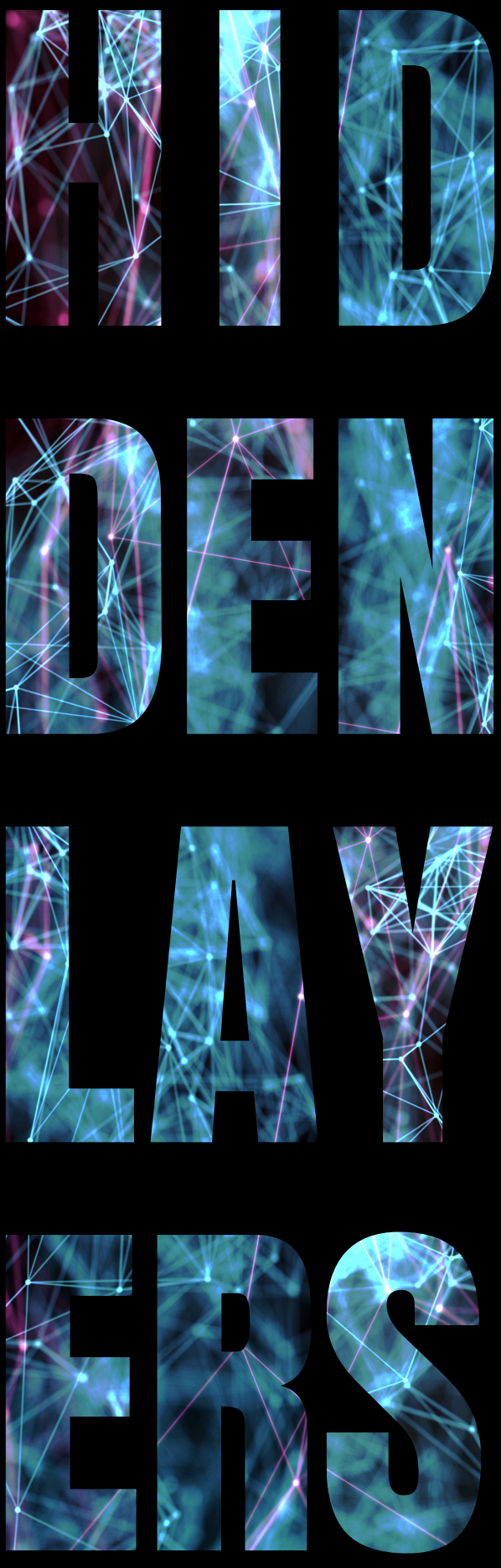
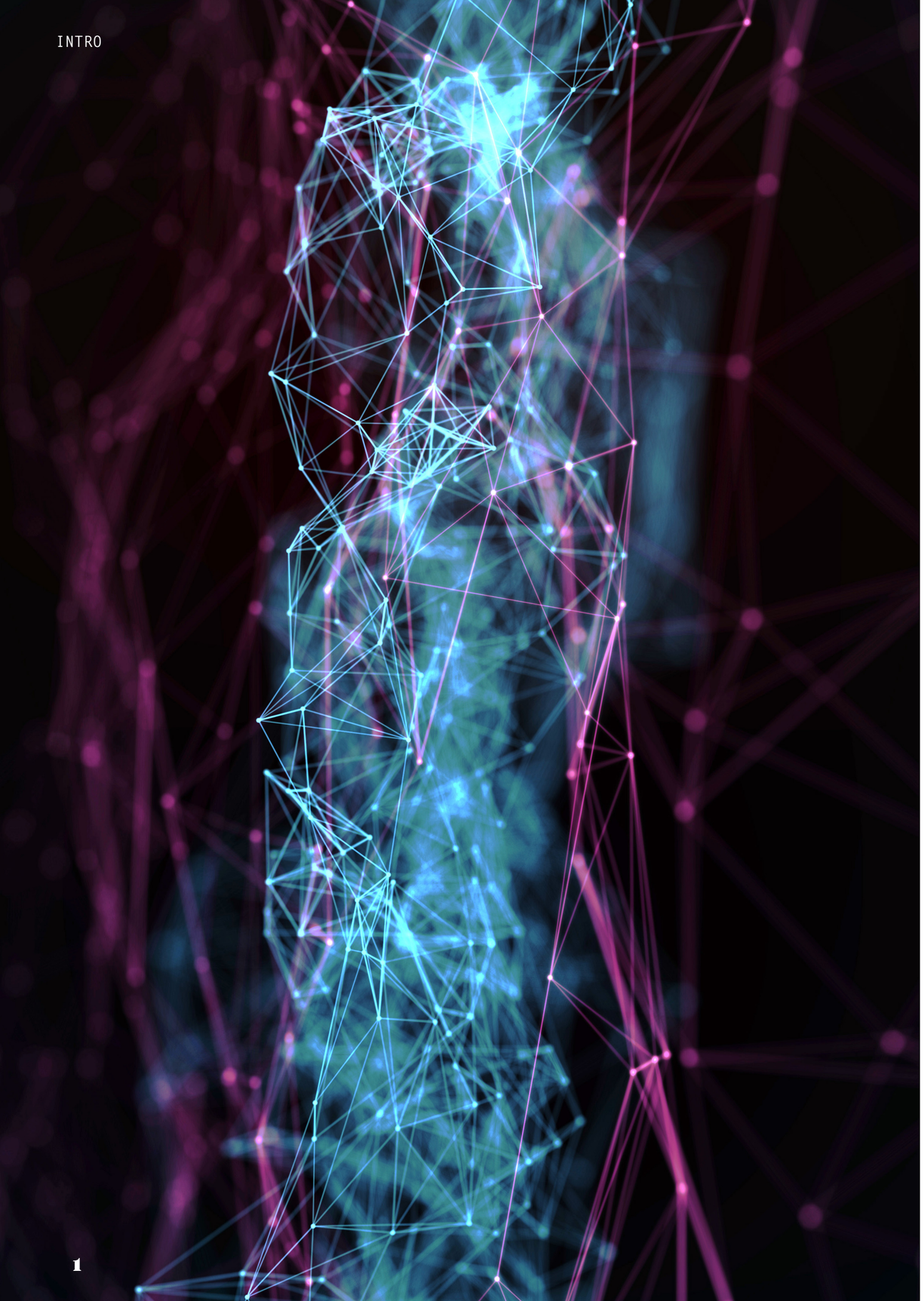
Bertelsmann
FOUNDATION




## YOUR QUARTERLY TRANSATLANTIC TECHNOLOGY NEWS

March 2024



Welcome back to another edition of Hidden Layers. In this issue, we discuss updates on the EU's AI Act, the Biden administration's AI executive order (EO) and a new AI task force from Congress. We also address the outcomes from the U.S.-EU Trade and Technology Council's (TTC) fifth ministerial meeting and a new EO to protect Americans' personal data.

# REGULATING AI

IN BRUSSELS

The November issue of Hidden Layers discussed the future of the EU AI Act and whether it would pass before the end of 2023. There was some skepticism about the bill's prospects for quick approval given disagreements among the member states on obligations for foundation models and exemptions for law enforcement use of AI, but the EU institutions swiftly reached a deal.

On December 8, after three days of trilogue negotiations, the European Parliament, the European Commission and the European Council reached a provisional agreement on the wording of the act. The legislation was finalized in early February after receiving unanimous approval from the 27 EU member states. The AI Act is undoubtedly a milestone in AI regulation that will have an impact on the global AI market and likely have a *de facto* Brussels effect, even if other governments and private-sector stakeholders disagree with its approach.

AI developers in markets beyond the EU, if they want to continue doing business in the bloc, will have to abide by Brussels' new rules. They may need to follow transparency guidelines and make changes to their business operations or AI models depending on the level of risk that the EU determines those models pose to European citizens. The act could also have a *de jure* Brussels effect, meaning the EU may inspire other governments to adopt similar legislation, as was the case with the EU's General Data Protection Regulation, which led to comprehensive data privacy laws in Japan and California.

The European Parliament must now hold a plenary vote, scheduled for March 13, to adopt the legislation. It would enter into force 20 days after its publication in the Official Journal of the European Union, which is likely to occur in June. Even then, however, the act remains unenforceable for another 24 months after its entry into force. That means companies will not need to comply until 2026, though prohibitions on unacceptable-risk AI systems will apply just six months after the act comes into force.

As the AI Act progresses through the European legislative process, the EU is already laying the groundwork for implementation. The bloc launched on February 21 a European AI office within the Commission's Directorate-General for Communication Networks, Content and Technology. The office will offer key implementation support to governance agencies in the 27 member states by establishing EU-level advisory bodies to promote information exchange. It will also help develop tools, methodologies and benchmarks for evaluating general-purpose AI models' capabilities and reach, classify models with systemic risks, and promote collaboration among leading AI stakeholders to create state-of-the-art codes of practice. Lastly, the office will investigate possible infringements of rules, conduct model capability assessments and request, when necessary, corrective actions from providers.

AT THE WHITE HOUSE

In the U.S., the Biden administration has made substantial progress implementing the president's AI EO signed in October of 2023. The White House issued in late January a 90-day update that outlined federal agencies' responses to the EO to strengthen AI safety and boost AI innovation. Some of these actions are:



## On AI Safety

- using the Defense Production Act to enforce requirements for developers of powerful AI systems to disclose information to the Department of Commerce about these systems, the computing clusters able to train these systems, and AI safety test results.

- proposing a draft rule to compel U.S. cloud companies that provide foreign clients with computing power for AI training to report such activities, thereby enhancing transparency and security measures.

- completing risk assessments of critical infrastructure sectors and ensuring the safe integration of AI into vital components of society, such as the electric grid. To reinforce the EO's whole-of-government approach to AI regulation, nine agencies are involved in this effort, including the Department of Defense, Department of Transportation, Department of Treasury, Department of Health and Human Services, and the Department of Homeland Security.

**On AI Innovation**

• launching the National AI Research Resource pilot program, managed by the U.S. National Science Foundation, to enhance broad-based innovation and competition, and ensure equitable access to AI research.

• launching an AI talent surge to accelerate hiring AI professionals across the federal government. The Office of Personnel Management has already granted federal agencies the authority to hire AI talent. It has also expanded programs that attract technological expertise, such as the Presidential Innovation Fellows, the U.S. Digital Corps and the U.S. Digital Service.

• introducing the EducateAI initiative to fund inclusive AI educational opportunities from the primary to the undergraduate level. The initiative aims to develop the AI workforce.

• funding new Regional Innovation Engines awards, such as those for the Piedmont Triad Regenerative Medicine Engine, which will receive up to $160 million over the next decade to advance AI-focused breakthroughs in clinical therapies and other fields.

• establishing an AI task force at the Department of Health and Human Services to develop policies for regulatory clarity and AI innovation in health care to address racial biases in algorithms, advance the development of drugs and improve health care delivery.

Following last November's AI Safety Summit in the UK, the U.S. also committed to establish an AI safety institute to conduct research and provide safety guidelines. U.S. Secretary of Commerce Gina Raimondo named in early February the key members of the executive leadership team that will lead the new institute, housed under the National Institute of Standards and Technology (NIST). She also announced the creation of an AI Safety Institute Consortium made up of more than 200 civil society organizations, academic institutions and AI providers, including several Big Tech companies. The consortium will support the development and deployment of safe and trustworthy AI, and issue guidelines for red-teaming, capability evaluations, risk management, and watermarking synthetic content.

DISCUSSIONS ON CAPITOL HILL

The House of Representatives launched on February 20 a bipartisan AI task force with 24 members. Led by Congressmen Jay Obernolte (R-CA) and Ted Lieu (D-CA), it will produce a report with policy recommendations and guiding principles so that Congress can ensure continued U.S. leadership on AI innovation and establish guardrails for developing safe and trustworthy AI. This is the chamber's first tangible measure to regulate AI after last year's series of hearings, including one with Open AI's CEO Sam Altman, on the technology and its risks. Although there is no set date for releasing the report, the task force aims to advance four to 10 major pieces of AI legislation this year.

Since February 2023, both houses of Congress have proposed approximately 70 AI-related bills. None have been approved, but several show promise. The CREATE AI Act, for example, is among the bills that the House's AI task force is trying to advance this year. This legislation establishes a National AI Research Resource to provide a shared national research infrastructure that will expand access to research, data and tools for developing trustworthy AI. The AI Literacy Act, introduced by Rep. Lisa Blunt-Rochester (D-DE) and Rep. Larry Bruschon (R-IN), recognizes the importance of education at all levels to maintaining national competitiveness. It proposes to amend the Digital Literacy Act by codifying AI literacy as a key component of digital literacy.

Lastly, the AI Research, Innovation and Accountability Act of 2023, introduced by Sens. John Thune (R-SD) and Amy Klobuchar (D-MN), is among the most widely discussed AI bills. It would establish a framework to bolster innovation while bringing greater transparency, accountability and security to the development and operation of the highest-risk AI applications, including those involving critical infrastructure. The act provides clear definitions for generative, high-impact and critical-impact AI systems, and the clarity is imperative to ensure that legislators and AI developers are using the same language. The bill's focus on transparency extends to large internet platforms, requiring them to notify users when the platform is using generative AI to create content the user sees. The bill also instructs NIST to develop recommendations for technical, risk-based guardrails for high-impact AI systems. NIST would consult with other federal agencies and private-sector stakeholders in this effort.

Congressional action on AI regulation will be pivotal in 2024. Without it, some Biden administration policies may lack enforceability. With it, the guidelines and best practices established by the EO cannot be quickly undermined by a new president if there is a change in administration after November.

COMMITMENTS FROM MUNICH

At the Munich Security Conference (MSC) on February 16, leading technology companies, including Adobe, Amazon, Google, OpenAI, TikTok and X (formerly known as Twitter), signed a Tech Accord. The agreement is a pledge to cooperate on preventing deceptive AI content from interfering with this year's many elections worldwide, including in India, Mexico, the U.S. and the EU.

The rise of generative AI and the widespread availability of large language models has given malicious actors, including governments, new, sophisticated tools that can undermine elections and the democratic process more broadly. To confront this challenge, the Tech Accord establishes a set of corporate commitments to deploy tools that detect and counter harmful AI-generated content designed to deceive voters. Signatories will also conduct educational campaigns, raise public awareness and track the origin of deceptive election-related content. The agreement, importantly, defines harmful, election-related AI-generated content as "audio, video, and images that deceptively fake or alter the appearance, voice, or actions of political candidates, election officials, and other key stakeholders in a democratic election, or that provide false information to voters about when, where, and how they can vote". This definition could be used across jurisdictions for regulating the use of AI in elections and political campaigns.

# U.S.-EU TRADE AND TECHNOLOGY COUNCIL (TTC)

The U.S.-EU TTC held its fifth ministerial meeting at the end of January to discuss issues of economic security, cooperation on critical and emerging technology, and sustainable trade.

On economic security, the council deliberated the importance of de-risking and diversifying the U.S. and EU economies and building resilient supply chains to avoid becoming too dependent on other markets. Also on the agenda was employing outbound investment mechanisms to safeguard national security-related technologies, specifically AI, semiconductors and quantum computing. Transatlantic coordination of export controls on semiconductors and other critical technologies will continue so that protections against the misuse of dual-use technologies can be maintained and "tech leakage" to China can be prevented.

The U.S. and EU have committed themselves to further expanding transatlantic cooperation on critical and emerging technologies, including AI, while promoting innovation, security and trustworthiness across digital ecosystems. During the recent TTC meeting, the partners welcomed the technology industry's U.S.-EU Beyond 5G/6G roadmap, which offers guiding principles and next steps for 6G technology development. The U.S. and EU also pledged to embrace the International Guiding Principles on AI and the voluntary Code of Conduct for AI developers adopted at the G7 summit. Lastly, the transatlantic partners celebrated the signing of the U.S.-EU Joint CyberSafe Products Action Plan, which aims to establish a unified marketplace with cybersecurity standards for internet-connected products.

Two stakeholder events took place following the TTC. One focused on semiconductor supply chains by addressing the state of the sector, strategies for improving supply chain resilience and transparency, and governmental measures to mitigate dependency on any one country for legacy semiconductors. The other stakeholder event centered on sustainable trade and considered ways to strengthen the transatlantic green marketplace by facilitating development of sustainable and net-zero economies. It featured a workshop on promoting quality jobs that support a successful green transition. Stakeholders exchanged best practices and discussed strategies for ensuring that climate policy and investment lead to such jobs.

The next TTC ministerial meeting in Belgium is scheduled for later this spring.

## ON PRIVACY

On February 28, President Biden issued an EO to protect Americans' sensitive personal data from exploitation by countries of concern, namely China, Cuba, Iran, North Korea, Russia and Venezuela. The EO creates safeguards against activities that could grant these countries access to Americans' personal data and empowers the attorney general to prevent large-scale transfers of such data.

The White House's statement argues that companies are collecting personal data more than ever before and legally selling it through commercial data brokers that then resell it to countries of concern, or entities controlled by those countries. This poses a national security concern as the data ultimately lands in the hands of foreign intelligence services, militaries or companies controlled by other governments. In the absence of federal data privacy regulation set by Congress, the EO directs the Department of Justice and other agencies, such as the Department of Homeland Security and the Department of Health and Human Services, to establish greater data protections. The EO focuses on the most sensitive personal information, including genomic, biometric, health, geolocation and financial data, as well as certain types of personally identifiable information.

Leaked sensitive personal data is already the issue of a lawsuit. On February 16, plaintiffs in California, Illinois, Massachusetts, New York and Virginia sued Chinese e-commerce company Temu for "purposefully and intentionally" loading its app with malware and spyware that allow access to personal data on users' phones. The complaint alleges that customers' credit card and bank information was sold or leaked. It also claims that the app requests at least 24 unnecessary permissions, including those for accessing Bluetooth, Wi-Fi network information and biometric data.

It is unclear at this time if Temu shares the information it collects with data brokers or China's intelligence service. Still, the allegation that the company sought to cut costs by repeatedly failing to comply with security standards may prove true. Temu is the subject of over 1,800 complaints, many of which are privacy related, to the Better Business Bureau despite being in business for only 17 months.