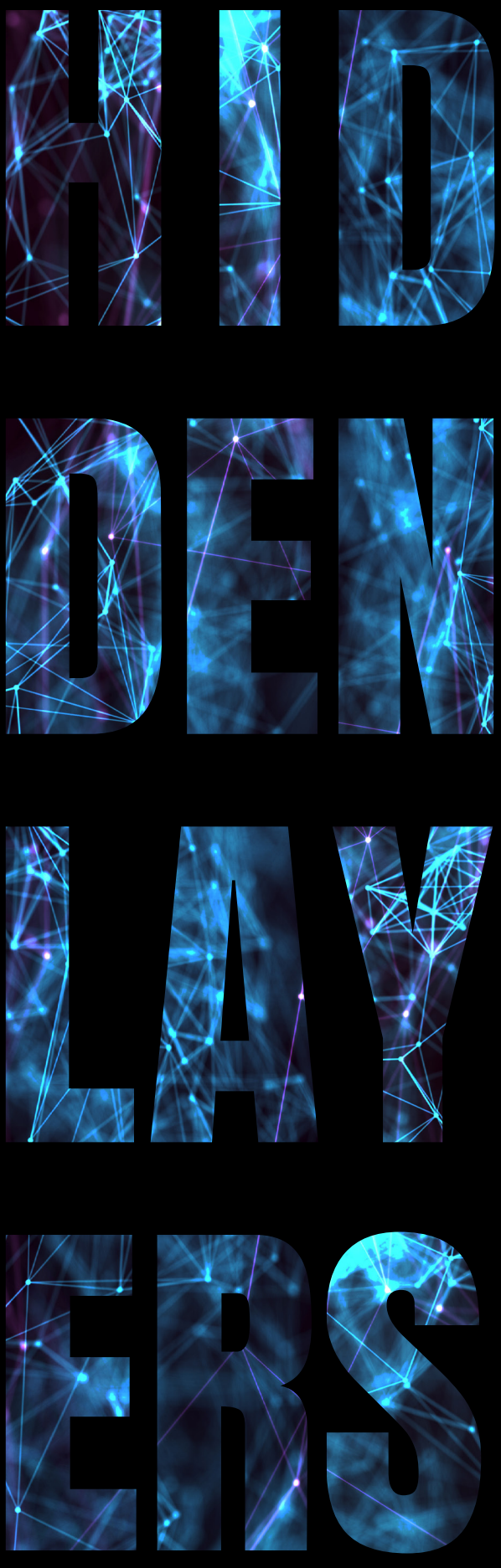
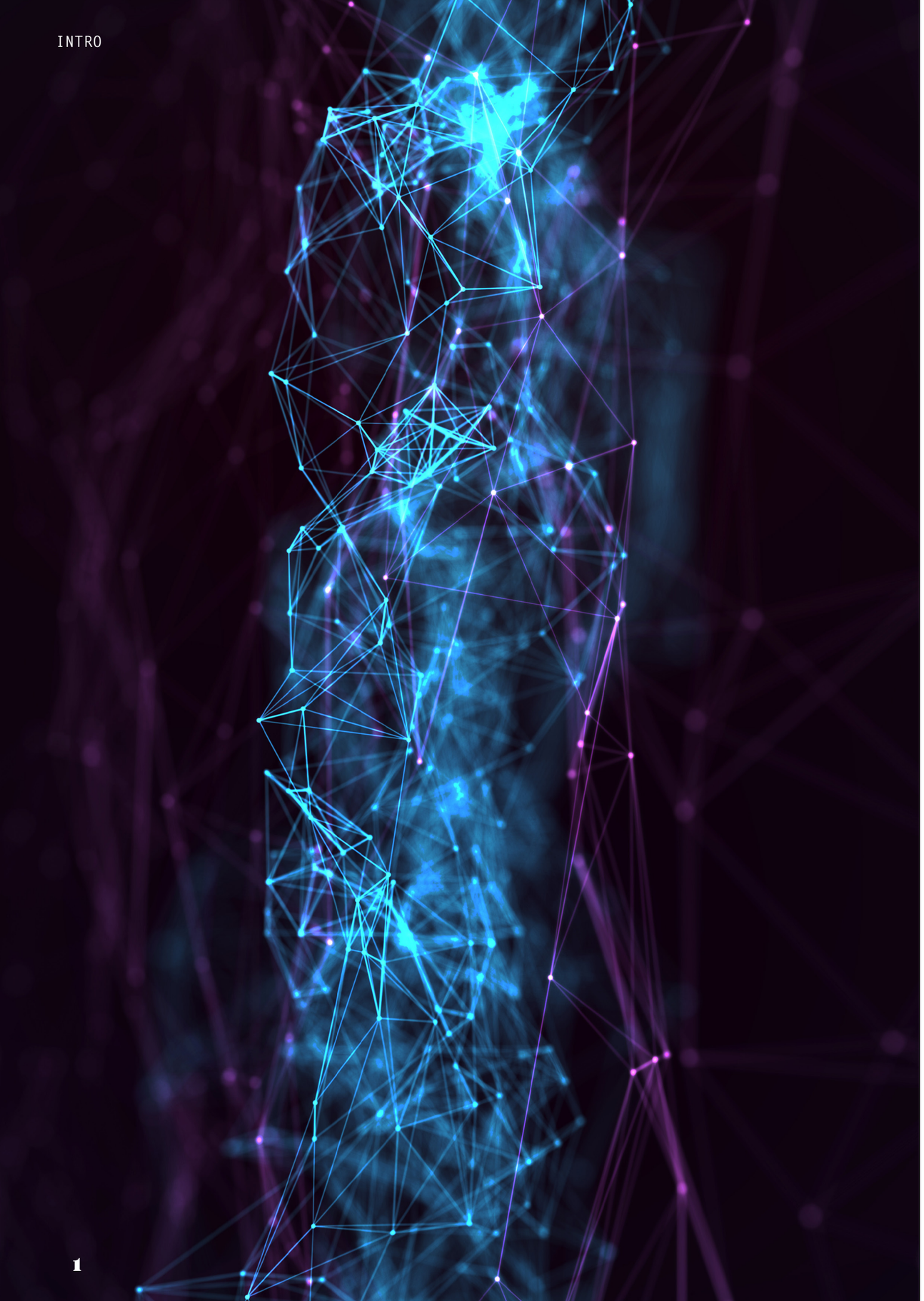
Bertelsmann
FOUNDATION



YOUR QUARTERLY TRANSATLANTIC TECHNOLOGY NEWS

August 2023



Welcome back to another edition of Hidden Layers. In this issue, we discuss AI regulation in the U.S. and the EU, a new adequacy decision from the European Commission on the Transatlantic Data Privacy Framework, the UK Online Safety Bill and the use of AI in hiring.

REGULATING BIG TECH

The rise of OpenAI's ChatGPT and the EU's concerns over data protection issues were highlights of Hidden Layers' April 2023 edition. Since then, the company's CEO, Samuel Altman, met with U.S. and European policymakers to advocate for generative AI and its benefits, but he also called for government regulation to mitigate risk. On May 16, Altman testified before the U.S. Senate judiciary committee and held private meetings with members of Congress and the Biden administration to "bridge the knowledge gap between Silicon Valley and Washington". Senator Richard Blumenthal (D-CT), who led the hearing, said it was refreshing to hear a top technology executive call for regulation and express his willingness to work with Congress rather than avoiding regulation as others have done.

Altman then traveled from Washington, DC to Europe to meet with European Commission President Ursula von der Leyen, French President Emmanuel Macron and UK Prime Minister Rishi Sunak to convey similar messages. The undertakings are strategic moves designed by OpenAI's public policy team to respond to policymakers' speculation and fear that generative AI could disrupt industries, displace workers, and exacerbate existing problems such as disinformation and the distribution of harmful content. The company aims to shape the debate on governance of a technology that is bound to be regulated at some point.

OpenAI has been particularly active on this front in Brussels, where the European Parliament voted on June 14 to adopt a negotiating position on the AI Act, the EU's risk-based approach to AI regulation, clearing the way for talks on a final version of the law with the European Council and the European Commission. ChatGPT's growing popularity led parliament to incorporate rules for generative AI in the new legislation, but, TIME Magazine reports, OpenAI has been proposing amendments and "lobbying to water down" the AI Act to reduce its regulatory burden. The company opposed in 2022 an amendment that would have designated general-purpose AI systems, such as GPT-3, as high risk, meaning these systems would be subject to strict transparency, traceability and human oversight requirements. OpenAI proposed that these requirements be placed not on the companies building general-purpose AI but those that use AI systems for high risk use cases, such as in employment or law enforcement. Parliament's final draft reflects OpenAI's position, but it does order AI providers to comply with smaller requirements, such as conducting risk assessments, preventing the creation of illegal content and disclosing if a system was trained with copyrighted material.

The EU, which wants to finalize the wording of the AI Act by the end of the year, is not alone in addressing AI governance. The Chinese Cyberspace Administration recently announced new regulations for the generative AI industry that will take effect on August 15. The rules, which make China one of the first countries to regulate the sector, encourage the innovative use of the technology but require service providers to conduct security reviews and register their algorithms with the government if their systems are capable of mobilizing the public.

Although Congress has not yet drafted any AI regulation on par with the EU's AI Act, several initiatives have been proposed. Senator Chuck Schumer (D-NY)

presented in June a "SAFE Innovation Framework" for AI policy that prioritizes innovation while establishing guardrails to ensure security, accountability, and explainability. Regarding security, Schumer's proposal focuses on preventing foreign adversaries, autocracies and domestic groups from abusing AI for financial gain or political upheaval, or threatening the security of the U.S. workforce. In a speech at the Center for Strategic and International Studies Schumer noted that AI, if ignored, could exacerbate the erosion of the middle class and impact workers ranging from the unskilled to those with advanced degrees. He also emphasized the need to protect the foundations of American democracy and to set AI norms before others do, explicitly mentioning the Chinese Communist Party.

In the House of Representatives, Congressmen Ken Buck (R-CO) and Ted Lieu (D-CA) introduced a bipartisan bill that proposes creating a national AI commission to review the United States' current approach to AI regulation, make recommendations on any new office or governmental structure that may be necessary, and develop a risk-based framework for AI. The commission will comprise experts from civil society, government and industry. On the other side of the Capitol, Senators Josh Hawley (R-MO) and Blumenthal introduced bipartisan legislation that would exclude generative AI from Section 230 immunity to ensure consumers have the tools to protect themselves from harmful content produced by generative AI. The senators said in a press release that this bill is a first step towards writing the rules for AI and preventing a repetition of mistakes made with applying Section 230 to Big Tech.

While Congress decides how to regulate AI, the White House reached on July 21 a non-binding agreement with seven AI companies—Amazon, Anthropic, Google, Inflection, Meta, Microsoft and OpenAI—on standards for safe, secure and transparent AI development. The companies agreed to eight rules, including internal and external testing of AI systems before their release, investing in cybersecurity and insider threat safeguards for unreleased models, using watermarks for AI-generated content, and researching AI's societal risks such as harmful bias and data privacy. These safeguards, while non-binding, will serve as primary guidance for companies; the White House will soon release a related executive order on AI.

ON PRIVACY

After the European Court of Justice (ECJ) struck down in 2020 the Privacy Shield framework that regulated data flows between the U.S. and EU, President Joe Biden and von der Leyen reached an agreement on a new Transatlantic Data Privacy Framework in March 2022. Seven months later, Biden signed an executive order to address EU concerns about U.S. intelligence agencies' collection of Europeans' personal data. The order committed Washington to strengthening privacy and civil-liberty safeguards for signals intelligence activities. It also allows EU citizens to seek redress if they believe the U.S. has violated their data privacy rights.

On July 10, after more than a year of negotiations, the European Commission adopted its adequacy decision for the new framework, thereby affirming that the U.S. ensures a level of protection for personal data transferred from the EU to U.S. companies that is comparable to the bloc's safeguards. The decision is an important step in restoring the safe and free flow of data across the Atlantic, a data transfer relationship worth $7.1 trillion. Max Schrems, the privacy advocate who led the campaigns against the first two U.S.-EU data transfer agreements, has already expressed concerns over the new one. He says that the latest agreed provisions are insufficient and that the new framework can be effective only with significant changes to U.S. surveillance law. Schrems may file his third legal challenge with the ECJ, but for the time being companies can rely on the new framework for data transfers.

Across the English Channel, the British parliament has been trying to pass the Online Safety Bill, which aims to regulate online platforms and make the internet safer, particularly for children. Since 2019, when the bill was originally proposed as an Online Harms White Paper, four prime ministers and five digital ministers have been in office, and the legislation has been broadened with multiple amendments, some controversial. Technology companies, security researchers, privacy advocates and civil liberties groups have heavily criticized the latest version of the bill for its privacy loopholes.

A recent amendment, for example, would allow the UK Office of Communications to require technology companies to scan for child sex abuse material in encrypted messages and authorize government backdoor access to any end-to-end encrypted system. This rule is problematic as end-to-end encryption is critical to ensuring privacy and safety on secure messaging apps, which is particularly important to journalists, human rights activists and diplomats. Meta's WhatsApp has spoken out against the bill, refusing to weaken its level of encryption even if that means UK authorities block the service. The Wikimedia Foundation has joined the fight against compliance, arguing that having to verify the age of British readers and contributors would violate its commitment to collecting minimal user data. The bill is nonetheless expected to become law by the end of the summer. A third and final reading in parliament is scheduled for September 6.

To learn more about the U.S.-EU data privacy agreement, watch *Privacy Shield 2.0 – The New Transatlantic Data Privacy Framework Explained*

TURNING TO AI

AI systems are being used across industries to improve productivity and efficiency by automating tasks. In many offices, these systems conduct human resources operations; more than 80% of employers use AI in some form to help screen applicants and make hiring decisions. Like most AI applications, however, the practice comes with risks. In 2022, the U.S. Department of Justice's Equal Employment Opportunity Commission (EEOC) issued guidance to employers on ways to ensure AI and other automated hiring tools do not violate the Americans with Disabilities Act by disadvantaging applicants with disabilities. The EEOC is working with federal agencies to ensure compliance with the guidelines, though they apply to employers nationwide.

A new New York City law, the first of its kind worldwide, aims to protect job applicants from algorithmic discrimination in the hiring process. The legislation requires companies relying on automated employment decision tools that use machine learning, statistical modeling, or data analytics to ensure a bias audit was conducted before the tool's use, post the audit results on their websites, notify job candidates and employees that AI tools are used in the hiring process, and include instructions for how to request an alternative selection process. The legislation aims to increase AI transparency and ensure companies can guarantee that their algorithms do not discriminate against gender or race.

Public interest advocates have criticized the law for not going far enough while private-sector representatives claim it is impractical. There is a fine line to walk and multiple interests to balance, as the EU has demonstrated with its efforts to regulate fast-developing AI technology. One challenge is implementing broad AI principles that fail to address specific uses. New York City is attempting to get around that by targeting a narrow AI application. The process will undoubtedly provide lessons from which other U.S. jurisdictions will learn as they draft their own regulation for using AI in hiring.