

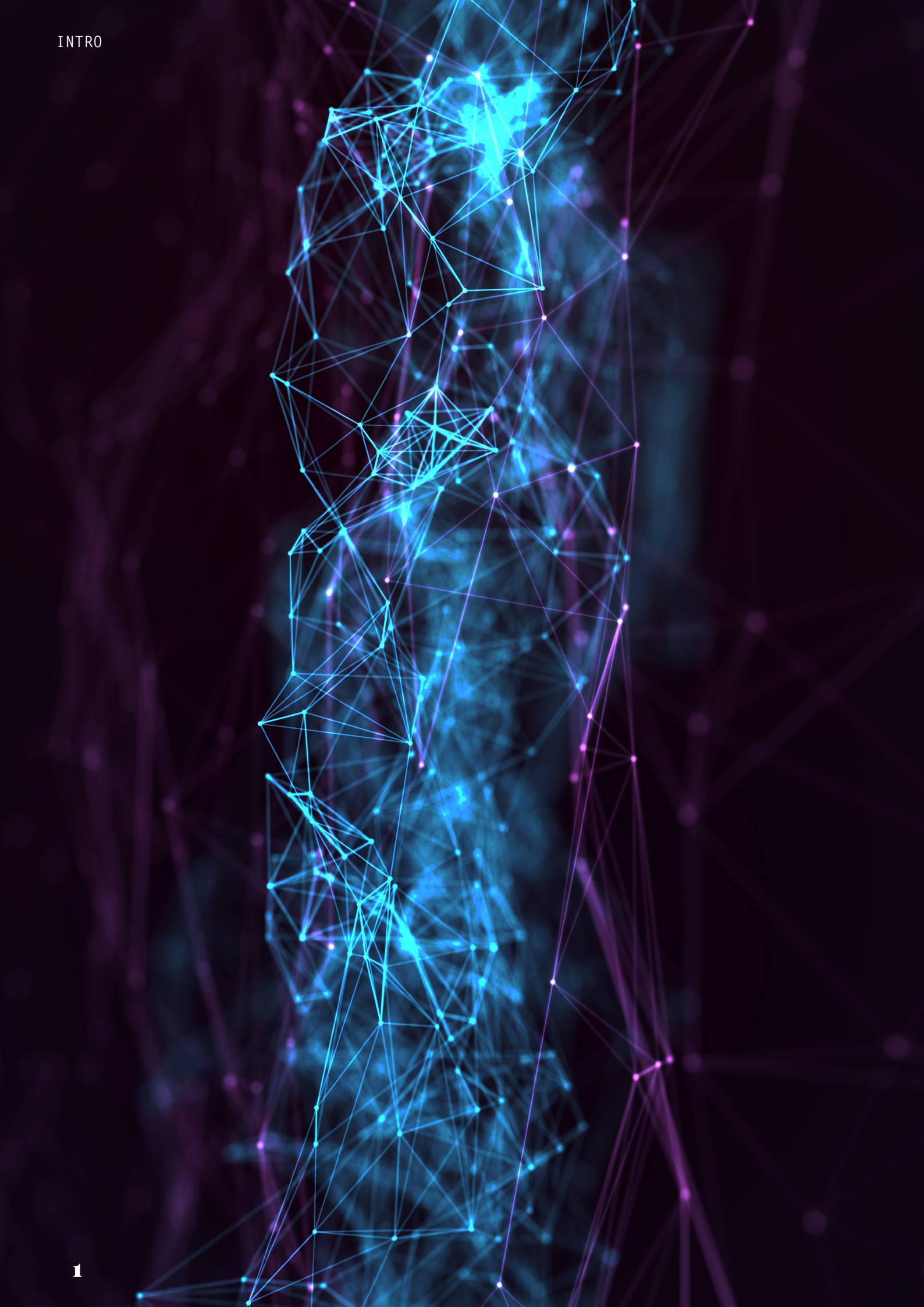
H
I
D

D
E
N

L
A
Y

E
R
S

YOUR QUARTERLY TRANSATLANTIC TECHNOLOGY NEWS
April 2023



Welcome back to another edition of Hidden Layers. In this issue, we discuss two cases heard by the Supreme Court at the end of February that may decide the future of Section 230. We also look at a bill from Congress that could ban Chinese apps such as TikTok from the U.S. market. Finally, we cover the White House's National Cybersecurity Strategy, the EU Data Act and the buzz around ChatGPT.

REGULATING BIG TECH

Section 230 reform was among the most important technology-policy debates when the 118th Congress first convened in January. This section of the Communications Decency Act came into force almost 30 years ago to give immunity to online platforms when third-party content generated by users violates the law. Section 230 was intended to help online platforms grow when the internet was in its infancy, but today's internet-based companies are among the world's largest and most powerful. Repeated calls from Congress, and the [Trump](#) and [Biden administrations](#), to reform, or even repeal, Section 230 to combat the spread of misinformation and harmful online content have fallen on deaf ears. No such measures have ever been taken.

At the end of February, Section 230's future was in the hands of the U.S. Supreme Court as it heard two cases, [Gonzalez v. Google](#) and [Twitter v. Taamneh](#), stemming from content posted by the terrorist group ISIS on Google's YouTube and on Twitter. The plaintiffs, who lost family members in the terrorists' attacks in France and Turkey, are accusing the platforms of aiding and abetting terrorism by taking insufficient action to identify and remove the content and, through their recommendation algorithms, subsequently promoting ISIS's videos. Both cases give the Supreme Court the opportunity to repeal Section 230 and fundamentally reshape the internet, but the justices, after hearing the plaintiffs' arguments, [appeared hesitant](#) to upend the law.

In the case of [Gonzalez v. Google](#), the plaintiff's counsel argued that YouTube's recommendations should be considered the company's own speech and, therefore, fall outside Section 230 protections. But this distinction

confused the justices because, they indicated, it blurred the line between YouTube and third-party content. [Justices Sonia Sotomayor and Clarence Thomas](#) were unconvinced by claims that the company was aiding and abetting terrorism through its algorithm because YouTube gives users suggestions based on content in which they have already expressed interest. [Justice Elena Kagan](#) added that the job to alter Section 230 might be better suited for Congress since the Supreme Court justices "are not the nine greatest experts on the internet".

The intertwining of national security and threats to privacy from foreign internet companies operating in the U.S. has been another priority for American policymakers. In early March, Congress unveiled the [RESTRICT Act](#), a bipartisan bill that gives the Department of Commerce and the White House new powers to ban or restrict a wide range of technology products from countries with adversarial relationships with the U.S., namely China, Cuba, Iran, North Korea, Russia and Venezuela. Since all but one of those countries lacks a thriving technology sector, it is clear the bill targets Chinese companies. The White House [endorsed the legislation](#), noting that it provides a framework for addressing technology-based threats to Americans' safety while creating new mechanisms for government to combat national security risks posed by certain foreign businesses operating in the U.S.

Two weeks later TikTok CEO Shou Zi Chew testified before the House Energy and Commerce Committee about the risks the app poses to children and teenagers, and its relationship with Beijing-based parent company ByteDance.



U.S. lawmakers are concerned about ByteDance's links to the Chinese Communist Party (CCP) and whether party officials can access data collected from TikTok's 150 million American users.

Chew downplayed the company's connection to China during the [hearing](#), emphasizing that it does not have offices in China or store data there. He noted that data is stored in his home country, Singapore, and that ByteDance "is not owned or controlled by the Chinese government.

It is a private company." Members of Congress appeared unmoved and pressed Chew about the CCP's golden share in ByteDance. In 2021, [The Information](#) revealed that the Chinese government quietly bought a minority stake and a seat on ByteDance's three-person board of directors. While the CCP does not own ByteDance, a board seat gives them significant insight into the company's inner workings and raises questions about the extent of Beijing's influence on ByteDance and the wider Chinese technology sector.

ON PRIVACY

The White House released in early March a [National Cybersecurity Strategy](#) to promote a safe and secure digital ecosystem and ensure the protection of citizens' data. The strategy seeks to shift responsibility for cyberspace defense from small businesses, individuals and local government to larger companies that are "most capable and best-positioned to reduce risks". The document also emphasizes long-term investment incentives that promote digital security and resilience, public-private collaboration, increased regulatory action and private-sector liability, and collaboration with allies. Its [implementation](#) would impact operators of critical infrastructure, software developers, cloud providers and businesses that handle personal information.

The strategy also aims to promote the protection of personal data and the security of Internet of Things (IoT) devices, which collect massive amounts of data and are often vulnerable to malicious cyber activities. As part of this privacy effort, the administration will support legislation that places clear limits on the collection, use and transfer of personal data or provides strong protections for sensitive data, such as geolocation and health information. It will also promote IoT cybersecurity through federal research and development, risk management efforts and IoT security labeling programs that allow consumers to compare the cybersecurity protections offered by different IoT products. The administration hopes that the labeling programs will create market incentives for more secure IoT devices.

As a follow-up to the National Cybersecurity Strategy and the second Summit for Democracy, the White House Office of Science and Technology Policy released on March 30 a [National Strategy to Advance Privacy-Preserving Data Sharing and Analytics \(PPSA\)](#). This second report acknowledges the many beneficial uses of data but also

the risks involved in sharing and analyzing it. The document provides a roadmap for public- and private-sector entities to use privacy-enhancing technologies appropriately and ultimately build a trustworthy data ecosystem that minimizes risks to individuals and society. In the absence of federal privacy legislation, the PPSA may be the second-best option. For the Biden administration, it is also an opportunity to demonstrate that it is making an effort to safeguard Americans' personal data.

On the other side of the Atlantic, the European Parliament [approved on March 14 the Data Act](#), legislation that aims to "boost innovation by removing barriers obstructing access by consumers and businesses to data". In other words, the act makes more data available for use, allows it to flow freely across economic sectors within the EU and establishes rules for data access. The EU claims the Data Act will contribute to the development of new services, especially artificial intelligence (AI) services that require large amounts of data to train algorithms, and will lead to cheaper maintenance and repair of connected devices.

The [U.S. Chamber of Commerce](#) has criticized the Data Act. The group argues that the new legislation will penalize competition, slow innovation, force companies to share trade secrets with competitors and EU government entities, and threaten American companies' ability to transfer data out of Europe. The European Parliament nevertheless overwhelmingly approved the legislation by a 500-23 vote. It is now on track to enter a final stage of negotiation between the parliament and the European Council. The Data Act follows the [European Data Governance Act](#) and is part of Europe's strategy to become "a leader in data-driven society".



TURNING TO AI

Discussions on AI this past quarter have focused mainly on natural language processing models such as ChatGPT, the new chatbot that quickly became a trending topic worldwide. San Francisco-based OpenAI launched ChatGPT in November 2022, and it quickly [set a record](#) for the fastest-growing consumer application ever, attracting 1 million users within a week and 100 million users within two months.

ChatGPT is trained to mimic human conversation by an algorithm called a [transformer](#), a type of neural network that learns context and meaning. The model undergoes multiple training stages with human annotators who rank the appropriateness of its responses until it can generate text that is almost indistinguishable from that from a human. Data is also key to the learning process. ChatGPT was trained using [570 gigabytes of data from books, articles, websites and other online texts](#). That's 300 billion words.

ChatGPT is a milestone in the field of conversational AI because its model can understand and analyze large amounts of natural language data, and recognize linguistic nuances. While traditional chatbots, such as Siri and Alexa, can follow only pre-defined templates, ChatGPT responds to a wide range of inputs and produces natural-sounding conversation. The technology has many applications, from virtual assistants to e-commerce and finance to healthcare. Real estate agents can use ChatGPT to write property descriptions. Health care workers can use it to summarize patient records. Writers can use it to draft movie scripts, and programmers can use it to write code.

ChatGPT offers many benefits and has the power to revolutionize industries as the model improves with user

exposure, but policymakers are skeptical of the technology. As ChatGPT gains popularity in the U.S., [members of Congress](#) are becoming more aware of AI's potential harm and are calling for regulation of the technology. They fear its potential misuse and impact on national security and education. Positive aspects aside, ChatGPT could be used to spread disinformation, and students could use it to cheat, leading educators to prohibit the use of computers and return to the days of the handwritten essay. Concern is also growing about AI systems conducting basic tasks better than humans can. Regulators argue that the social implications are enormous, especially if the technology begins to displace workers.

European regulators worry about ChatGPT's potential impact on data privacy. The Garante, Italy's data protection authority, [issued on March 31 an immediate temporary ban on ChatGPT](#) following a data breach of some users' conversations and payment information. Italian regulators [criticized Open AI](#) for not informing users about its collection of personal data and noted the lack of a legal basis for collecting and storing the data. Since Italy claims ChatGPT is in breach of the EU's General Data Protection Regulation, temporary bans by other member states or at the EU level may follow. Shortly after Italy's ban, [Reuters reported](#) that privacy regulators in France and Ireland are in contact with the Garante to learn more about the basis of the ban. The [European Data Protection Board](#) has also been evaluating the issue and announced on April 13 that it will launch a dedicated task force to exchange information on possible enforcement actions and foster cooperation between the different European data protection authorities.

The Garante has now given OpenAI a [list of measures](#) they must adopt by [April 30](#) in order to lift the ban, including publishing an information notice detailing its data processing, verifying users' age to ensure minors are not accessing inappropriate content on ChatGPT and clarifying the legal basis the company is claiming for processing the data. OpenAI must also allow users to exercise rights over their data and the ability to object to the data processing for the purpose of training its algorithms.

What do you think is the future of ChatGPT in Europe? [Submit your forecast on RANGE](#), the Bertelsmann Foundation's crowdsourced forecasting platform focused on transatlantic issues.