

HIID

DEEN

LAY

ERS

**YOUR QUARTERLY TRANSATLANTIC TECHNOLOGY NEWS**  
June 2022



Welcome back to another edition of *Hidden Layers*. In this issue, we discuss tech legislation making headlines in the first half of 2022, including the EU's Digital Markets Act (DMA), Digital Services Act (DSA), Digital Governance Act (DGA), and the U.S. Congress' proposed Digital Platform Commission Act. We also cover the latest on the U.S.-EU Trade and Technology Council meeting in France, the new transatlantic data transfer agreement, and the use of AI to interpret human emotion.



## REGULATING BIG TECH

The EU is moving quickly in the first half of 2022 to advance its proposed Big Tech legislation, starting with the European Commission's adoption on March 24 of the [Digital Markets Act \(DMA\)](#). The DMA bans large platforms acting as "gatekeepers" from using unfair business practices in the online marketplace. The EU defines gatekeepers as platforms active in at least three EU countries with a turnover of at least [€6.5 billion and more than 45 million monthly active end users](#). For companies that do not meet the quantitative threshold, the DMA allows the European Commission to investigate and designate a platform as a gatekeeper based on other factors such as use of the lock-in effect. Implementation is not expected until 2023 as the act still needs approval by the European Parliament and EU member states. The approval process takes 18 months on average, but the DMA is controversial among tech companies and may take even longer to become law.

One month later, on April 23, the European Commission and the member states reached a political agreement on the DMA's sister legislation, the [Digital Services Act \(DSA\)](#). While the DMA regulates the online marketplace and antitrust practices, the DSA focuses on platforms and content moderation, ensuring accountability and protecting EU citizens from harmful and illegal online content. The DSA allows the European Commission to supervise very large platforms, those (like gatekeepers) with a reach of more than 10% of the EU's 450 million consumers, and levy fines of up to 6% of global turnover or ban companies from operating in the EU single market in cases of repeated violations. The European Parliament and the European Council now must formally approve the agreement and adopt the legislation. A European Commission [press release](#) noted that the DSA, once adopted, will apply 15 months

after it enters into force or from January 1, 2024, whichever comes later. DSA terms will apply earlier to online platforms and search engines the European Commission designates as very large. For them, the act will come into force four months after the designation is made.

As the U.S. tries to catch up with the EU, several initiatives are under consideration in Congress. One is the [Digital Platform Commission Act](#), which Senator Michael Bennet (D-CO) introduced on May 12. This legislation would create an expert federal body to provide "comprehensive, sector-specific regulation of digital platforms to protect consumers, promote competition, and defend the public interest". The senator acknowledges that the U.S. has benefited from being the home of the world's leading tech companies. But he argues that the tech sector has amassed too much power over the American economy and democracy, and has been left to regulate itself for far too long. A new Digital Platform Commission, comprising five commissioners appointed by the president and confirmed by the Senate, would have the authority to develop and enforce rules, impose civil penalties, hold hearings, conduct investigations, and support research. It would also designate certain digital platforms as "systematically important", subjecting them to additional oversight, regulation, and merger review.

[Representative Peter Welch](#) (D-VT), who has been working closely with Senator Bennet to create the Digital Platform Commission, introduced on May 19 in the House of Representatives an identical bill. Representatives Lori Trahan (D-MA), Adam Schiff (D-CA) and Sean Casten (D-IL) floated a similar [proposal at the end of February](#). Rather than establishing an independent agency, their bill promotes a new platform-regulation bureau within the

Federal Trade Commission (FTC). [Politico reports](#) that Welch drifted away from this idea because he believes that a new bureau could overwhelm an agency already beset with too many responsibilities and interfere with its current work. If his bill is to move forward, Welch needs to find cosponsors in Congress and schedule a House Energy and Commerce Committee hearing.

To protect children on the internet, Senators Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN) [proposed](#) on February 16 the [Kids Online Safety Act \(KOSA\)](#). This bill requires social media companies to give users aged 16 or younger the option to disable addictive product features and opt out of algorithmic recommendations. It also gives parents more control over their children's social media usage, requires a yearly independent audit to assess social

media's risk to minors, and allows academics and public interest organizations to use company data to inform their research on children's internet safety. Opponents of the bill, such as the [Electronic Frontier Foundation](#), argue that KOSA puts children under surveillance from their parents and limits their access to information.

On antitrust, the Department of Justice endorsed on March 28 Senator Amy Klobuchar (D-MN) and Senator Chuck Grassley's (R-IA) [American Innovation and Choice Online Act](#). [Axios notes](#) that the endorsement gives the bill a boost and shows that the agency thinks the bill is enforceable and can increase tech competition in the U.S. The act, similar to the EU's DMA, would target Big Tech for consumer choice violations.





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

The TTC held its second ministerial meeting in Paris on May 15-16 to review the progress made by working groups since the previous ministerial meeting in September 2021. One main takeaway from the most recent gathering is the unsurprising shift in TTC priorities towards U.S. and EU cooperation against Russian aggression and information manipulation. [A joint statement](#) explicitly mentions Russia 56 times, while other strategic competitors such as China are only mentioned three times. The cohesive and effective transatlantic response to the war in Ukraine in the form of imposing sanctions and export controls on Russia has also led TTC working groups to focus efforts on finding areas in which the U.S. and EU can work together in future crises. Both sides recognize a common threat and the need for cooperation in perilous times.

Regarding technology, the [White House](#) reported on May 16 some key outcomes from the recent TTC discussions. These include:

- Greater information exchange on exports of critical U.S. and EU technology, with an initial focus on Russia and other potential sanctions evaders
- A joint roadmap on evaluation and measurement tools for trustworthy AI and risk management, and a common project on privacy-enhancing technologies
- A U.S.-EU Strategic Standardization Information (SSI) mechanism to enable information sharing on developments in international standards
- An early warning system to better predict and address potential semiconductor supply chain disruptions, and

discussion on a transatlantic approach to semiconductor investment

- A new cooperation framework for issues related to information integrity in crises, particularly on digital platforms, with a focus on Russia's information manipulation and censorship

- A policy dialogue aimed at developing responses to global food security challenges caused by Russian aggression in Ukraine, and a [U.S.-EU guide](#) to cybersecurity best practices for small- and medium-sized enterprises, whose businesses are impacted disproportionately from cyber threats



## ON PRIVACY

While visiting Brussels on March 25, U.S. President Joe Biden reached agreement with European Commission President Ursula von der Leyen [on a new transatlantic data privacy framework](#) that aims to reestablish a legal mechanism for the transfer of personal data. U.S. and European negotiators had discussed the details of this agreement for more than a year, since the previous transatlantic data transfer agreement, the U.S.-EU Privacy Shield, was rendered invalid by the EU's Court of Justice in July 2020. The next step is to translate the political agreement into legal documents that both sides can adopt. President Biden will have to sign an executive order outlining new U.S. commitments to privacy, allowing the Commission to determine if the measures are adequate.

The EU has also made progress on data governance. On March 21, the [European Data Protection Board \(EDPB\)](#) released a set of guidelines to assess and prevent dark-pattern practices on social media platforms that violate the General Data Protection Regulation (GDPR). The EDPB defines dark patterns as “interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data”. The guidelines outline principles for transparency, accountability, and data protection by design, and cite relevant GDPR provisions that can help assess dark patterns. The EDPB accepted public feedback on the guidelines until May 2.

On May 16, the Council of the European Union [approved the Data Governance Act \(DGA\)](#), which provides companies or individuals increased access to protected public-sector data for research and development of new products and services.

The DGA also creates safeguards for the international transfer of non-personal data. Similar measures are already in place for personal data under the GDPR. The new rules will apply after a 15-month grace period, which begins 20 days after the Official Journal of the European Union publishes the legislation.

To learn more about the U.S. and EU's new transatlantic data transfer agreement, look out for the Bertelsmann Foundation's *Privacy Shield 2.0 Explained* animation to be released this summer.





## TURNING TO AI

As the development of AI continues to advance at an extraordinarily rapid rate, machines are becoming increasingly sophisticated and gaining new skills. Policymakers may not be prepared for the implications of these developments. According to [MIT](#) research, machines have learned to recognize, interpret, and react to human emotions. This technology, called emotion AI, senses emotions through text, voice recordings, and video. Interpreting human emotion is difficult, but a machine's ability to analyze large amounts of data allows it to recognize small inflections in the human voice and facial microexpressions that the human eye would find difficult to discern. A computer then correlates this data with signs of anger, stress, or sadness.

Corporations have noticed the value of this technology and are already using emotion AI to improve product advertising, call centers, mental health services, and, by analyzing a driver's emotional state, even vehicle safety. The emotion-recognition sector is estimated to grow into a [\\$37 billion industry by 2026](#). But is it ethical for companies to use machines that constantly analyze consumers' emotional states? Could governments employ such technology for law enforcement or public safety? Is it more ethical to notify a consumer when such technology is in use or for the consumer to explicitly provide consent? European and American regulators have yet to provide comprehensive answers to these pertinent questions.

The EU's AI Act, proposed by the European Commission in 2021, is the world's most comprehensive AI legislation and addresses many risks posed by AI technologies. But the act does not deal with emotion recognition sufficiently. It requires only that companies or agencies deploying emotion-recognition technology inform the data subject

and be transparent about the technology's use. The EDPB argues that that is not enough. The board and the [European Data Protection Supervisor \(EDPS\)](#) believe the use of emotion AI should be prohibited in the EU, except in specific cases, such as in health care, when patient emotion recognition is important. The European Commission must now consider this feedback. The U.S. Congress, too, needs to look at regulating emotion AI alongside the use of facial recognition and other biometric technologies.