AEI Digital Platforms and American Life Project

The United States' Tech Regulatory Dilemma—Through a Foreigner's Eyes

Lilla Nóra Kiss

MARCH 2023

AMERICAN ENTERPRISE INSTITUTE

Executive Summary

This report addresses the United States' regulatory conundrum with tech companies, from the viewpoint of a foreigner. The big question is whether Congress should create a new industry-specific regulatory system for digital platforms. Specifically, the question is whether regulation enforcement should continue through the adjudication of antitrust laws via the court system or whether it should be taken up by, for instance, the Federal Trade Commission (or other—maybe new—agencies). The former would stand firmly with the traditional limited-government approach, while the latter would be an expansion of the administrative state. If the US adopts the latter, it will follow a regulatory approach that is common in Europe instead of following its typical free-market approach.

Finding the balance between regulation and non-regulation is no easy feat. Legislators often turn to adopting laws as their most effective tool, yet each reform poses the risk of unintended consequences. It's a delicate dance to navigate the chasm between regulatory and free speech "absolutism." This challenge is compounded by the fact that tech regulatory issues are complex, spanning multiple legal fields from antitrust to constitutional law, via criminal law and media law. Given these obstacles, the EU's proactive approach may provide a valuable road map as the US plays catch-up.

The regulatory dilemma is much broader than what meets the eye, as tech regulation also includes safeguarding national security in the digital realm through ensuring data security and preventing cyberthreats and cyberattacks. Furthermore, the emergence of social media platforms and their widespread use have led to a host of challenges in terms of managing IT. The use of social media for disinformation, propaganda, and manipulation has been a growing concern in recent years, and many governments are struggling to come up with effective solutions to combat these challenges.

Overall, the regulatory challenges faced by the tech industry are complex and multifaceted and require careful consideration and collaboration among governments, regulatory agencies, tech companies, and other stakeholders. Balancing individual privacy rights, national security interests, and innovation will continue to be an ongoing challenge as technology continues to evolve and shape our lives in new and unforeseen ways.

The United States' Tech Regulatory Dilemma—Through a Foreigner's Eyes

Lilla Nóra Kiss

Tech regulation is tricky, and the EU and US have taken vastly different approaches. While the EU tends to jump in headfirst, the US often takes a wait-and-see approach. It is a classic dilemma of "the early bird catches the worm" versus "the second mouse gets the cheese." But as with most things in life, timing is key, and understanding the nuances of these contrasting strategies is crucial to navigating the ever-evolving tech landscape.

The US is at a historical crossroads and must decide whether to regulate tech companies' activities. The question is whether enforcement should continue through the adjudication of antitrust laws via the court system or whether it should be taken up by, for instance, the Federal Trade Commission. The former would stand firmly with the traditional limited-government approach, while the latter would be an expansion of the administrative state.

In other words, the US has to decide if it will follow the European Union's path in adopting digital laws to limit the emerging powers of digital platforms or if it will stand firmly by its existing pro-competition legal frameworks supporting the free-market approach. In either case, European laws have an extraterritorial effect, often referred to as "the Brussels Effect,"[1] and will influence US tech companies.

The "how to handle digital platforms" dilemma oscillates between seemingly completely opposite extremes, from free speech absolutism to regulatory absolutism. On the one hand, platforms are blamed for banning free speech via their voluntarily made "editorial decisions,"[2] presumably protected under Section 230 of the Communications Decency Act of 1996.[3] On the other hand, platforms are private actors whose editorial decisions are arguably expressions of free speech themselves and thus protected by the First Amendment. One's conclusions on regulating digital companies depend on one's political, economic, or legal perspectives. Nevertheless, some main ideas determine the regulatory attitude.

Coming from a generally overregulated European legal culture, I understand the need for some kind of legal framework to keep power (in this case, private power) limited,[4] actors accountable, and activities somewhat predictable—and I do not consider regulation to be inherently wrong. However, after living in the US and watching the highly competitive tech market from the front row, I realize the picture is more nuanced. The regulatory dilemma is part of a bigger, more political and ideological battle. The outcome will determine the future, in both economic and constitutional dimensions.

As a foreigner, it would be difficult and irresponsible of me to either suggest the adoption of a comprehensive regulatory approach for digital platforms or encourage the US legislators to refrain from doing just that. The question of how to handle digital platforms in the US is a complex and multifaceted issue that involves balancing the need for regulation with the desire to protect free speech and competition. The EU's approach to regulating digital platforms offers valuable insights and considerations, but ultimately,

the decision about how to handle digital platforms in the US will depend on legislators' political, economic, and legal perspectives.

Juggling Public Interests

In the digital age, tech regulation poses a complex and multidimensional challenge for governments and policymakers worldwide as it is at the crossroads of multiple, seemingly colliding national and public interests. Balancing the need for regulation and national security with the desire to protect free speech, competition, and economic interests is a delicate task that requires careful consideration of multiple perspectives and competing interests.

Navigating Constitutional Status, Political Intentions, and Economic Interests. First, US leaders have to decide if they will preserve the existing framework for competition enforcement through the court system[5] or instead move toward a stronger administrative state, increasing the role of agencies and government actors while limiting corporate freedoms. Delegating the issue to administrative agencies might have been the default approach in earlier decades, but American judges, legislators, and lawyers have a newfound appreciation of the constitutional problems with excessive administrative discretion. Instead, Congress should take the lead in legislating the legal framework for these issues; agencies and courts will always have important roles to play, but they should be secondary to Congress itself.

The decision to regulate the tech industry is closely tied to legislators' political perspectives. Those who are more pro-regulation in general would likely favor a stronger role for the state in regulating the tech industry, while those who are more libertarian would likely favor a more hands-off approach and a smaller role for the government. The balance between regulation and free-market principles is a key consideration.

Tech regulation is a question of national economic interest. "Letting the market work" may increase competition that leads to innovation, economic growth, and consumer welfare, which all are obviously national interests for any capitalist country.[6] Therefore, from an economic point of view, maintaining the current (unregulated) status quo seems beneficial.[7]

Tech regulation is a question of national economic interest.

Refraining from tech regulation fits well with the constitutional concept of limited government—accepted more broadly in America—and the upholding of checks and balances between different branches of power. There is ongoing debate regarding the balance between economic interests and constitutional principles, with some advocating for a laissez-faire approach and others emphasizing the importance of oversight from legislators, regulatory agencies, and the judiciary. Legislators may adopt rules and agencies may adopt guidelines to promote particular national interests (e.g., consumer welfare). At the same time, the judiciary must evaluate how those decisions affect specific actors (businesses, consumers, etc.).

This constitutional structure of limited government and the economic attitude of limited intervention have coexisted for a long time in America. Changing either might depend on the contemporary political interests of the ruling party.

Protecting National Security and Defending Against Foreign Influence. Tech regulation also encompasses the broader public interest of national security in the digital realm, including the need to address cyberthreats, enhance data security, and prevent cyberattacks.[8] Tech innovation has opened Pandora's box in security matters, introducing a new potential battlefield in cyberspace. Users' privacy and data protection are one front of this battle, while the need for corporate- and state-level transparency and accountability are another. Decreasing vulnerabilities is in everyone's mutual interest.

Defense against data breaches and cybercrimes is vital because these attacks can result in financial damage, the loss of sensitive personal information, and disruption to critical infrastructure.[9] For example, a data breach at a major financial institution could result in losing billions of dollars and compromising sensitive financial data. Similarly, a cyberattack on critical infrastructure such as a power grid or water supply system could have devastating consequences for a country's citizens. As a result, governments must prioritize defense against these types of attacks to protect their citizens and maintain national security.

Additionally, reducing cyberthreats in general is important because it helps create a safer and more secure online environment for all individuals and organizations. Cyberattacks happen every day all over the world and reach various industrial sectors, including education, telecommunication, health care, and public administration.[10] Thus, digital security needs new ways of preparation and alternative methods of investigation, compared to traditional law enforcement methods.

One priority is to reduce the possibility of potential cyberattacks on state institutions and private corporations. The question is whether this could be achieved under the existing material and procedural legal framework or whether new rules are needed to address such challenges. If new rules are required, careful examination is needed to reveal which legal field should be reformed and how to achieve the best results and avoid possible unintended consequences.[11]

Avoiding foreign influence and reducing potential espionage activities in the digital sphere are more challenging than in the physical world. The first and probably best-known example is the bipartisan concern about Chinese consumer technology.[12] President Donald Trump's executive order attempting to ban TikTok in 2021 warned that the app's

> data collection threatens to provide the Government of the People's Republic of China (PRC) and the Chinese Communist Party (CCP) with access to Americans' personal and proprietary information—which would permit China to track the locations of Federal employees and contractors, and build dossiers of personal information.[13]

President Joe Biden rescinded the executive order but announced a replacement to evaluate whether several foreign-controlled applications could pose a security risk to Americans and their data.[14] There is no evidence, however, that anything would prevent China (or others) from buying personal data if TikTok were American-owned.[15] This is mainly because US data protection laws are less elaborate and comprehensive than the EU's General Data Protection Regulation (GDPR)[16] and the conditions of the EU-US Privacy Shield—a framework for transatlantic data flows adopted in 2016 that is applicable only to US-EU relations.[17]

Another example of a national security threat is platforms' geopolitical potential, especially during wartime. Since Russia (re)started its war in Ukraine in February 2022, social media platforms have been used to reach the citizens of those countries.[18] For instance, Meta, which operates Facebook and Instagram, introduced safety features in Ukraine and Russia to protect users, which can be seen as a well-intentioned humanitarian move.[19] In addition, Meta has established a "special operations center" staffed by experts from across the company, including native Russian and Ukrainian speakers, who monitor the platform and take extensive steps to fight the "spread of misinformation."[20] The special operations center also intends to implement more transparency and restrictions around state-controlled media outlets.

This is not the first time Meta has used a specialized team to respond to a geopolitical crisis. In August 2021, it used a group of experts to monitor Taliban-related content after the Taliban seized power in Afghanistan.[21] In February 2021, Meta removed the main page of the Myanmar military for violating its rules on incitement to violence.[22] The company said in 2018 that it had failed to curb hate speech and misinformation in Myanmar that fueled attacks on the Rohingya Muslim community there.[23]

However, maintaining public order and security is the role and task of a (nation) state—not unelected private entities. Social media platforms are

not entitled to decide what is "good" or "bad" content; their choices are voluntary ones made by a private company and are not based on any legitimate authority.

The support Meta gives its users by allowing them to hide themselves and their acquaintances from their enemies could be seen as an excellent way to use social media. However, what if platforms decided to provide such technical support for the invaders—for example, to reveal the location of platform users? A platform and its home government may have different perspectives on what counts as a good use of data when it comes to national security. One thing is sure: These decisions have a significant public effect, though they are made based on private considerations and without legitimate authority derived from popular election or law.

In this form, the decisions might be supported by platform owners' moral obligations to "do good" with their assets, though their profit-oriented nature may affect their ability to act solely based on moral and ethical convictions (if any).[24] Adam J. White points out in an eye-opening article, "There has always been more to Google's mission ["Don't Be Evil!"] than merely helping people find the information they ask for." Although Google's mission of making information "accessible and useful" "sounds value-neutral . . . one has to ask: Useful for *what*? And according to *whom*?"[25] (Emphasis in original.)

There are no common standards for defining "good," and as mentioned, platforms act voluntarily when they attempt to do so. The big question is to what extent they are free to do that. In other words, what are the standards for platforms to determine "good" in their private spheres (within their autonomy in self-regulation), knowing that these concepts and principles affect life outside the platforms as well?

Can Americans Have Their Cake and Eat It Too? To put it simply, do these public interests collide? Does the legislature have to decide which is more important, promoting economic welfare or attempting to secure the internet? How can one measure, if at all, the prevalence of one to the detriment of the other? Overall, while these public interests may seem to be in conflict, they could be reconciled without tilting the balance of the branches of power.

Strategic Planning: Observing Europe?

The EU and the US have different approaches to regulating the digital economy, but they inevitably influence each other. Therefore, two particularly significant technical and legal externalities must be considered when designing regulations.

First, tech innovation (and its potential regulation) has spillover effects in other sectors of the economy. Thus, adopting certain rules around tech regulation may trigger unintended consequences elsewhere.[26] Therefore, designing any digital rules necessitates broad social consensus and cautious planning.

Second, tech innovations and state-level regulatory solutions reach across national borders due to the transnational features of digital markets. Since rules adopted in one jurisdiction (e.g., in the European Union) will necessarily affect others (like the US), strategic planning is needed to find the best possible legislative solution. As mentioned, the rules adopted in the EU to promote and support the "proper functioning" of the single market have extraterritorial legal effects. This is the so-called Brussels Effect, defined by Anu Bradford.[27] The Brussels Effect shows how the EU affects business globally "by promulgating regulations that shape the international business environment, elevating standards worldwide, and leading to a notable Europeanization of many important aspects of global commerce."[28]

That is why, regardless of US regulatory movements in the tech industry, the EU's legislative machine will influence the US system, because American digital companies operate in the EU, which is vital to consider with strategic planning.

The EU has a more comprehensive and proactive approach to shaping policy in areas such as data privacy, consumer health and safety, environmental protection, antitrust, and online hate speech. For example, the EU has already adopted the GDPR (a regulation, replacing the former directive) to

provide a higher level of protection to citizens' personal data. In addition, the EU established the Privacy Shield framework with the US to regulate transatlantic data flows.

Recently, the EU has adopted the Digital Services Act and the Digital Markets Act under the Digital Single Market strategy umbrella—that is, an effort to give Europeans access to information and commerce across borders while maintaining strong consumer-protection requirements.[29] The Digital Services Act proposes to upgrade liability and safety rules for digital platforms, services, and goods and take further steps toward completing the Digital Single Market. The Digital Markets Act addresses the negative consequences arising from certain behaviors by platforms acting as digital gatekeepers to the single market. Its political ambition is "[to ensure] fair and open digital markets."[30] The proposals are ambitious and in line with the EU's intentions to lead digital legislation all over the globe and strengthen its digital sovereignty.[31]

In contrast, the US has a more hands-off approach to regulation, focusing on promoting competition and innovation in the tech industry. The Federal Trade Commission and the Department of Justice are responsible for enforcing antitrust laws and protecting consumers. However, there have been calls for more comprehensive regulation in the digital sphere, particularly regarding data privacy and online hate speech.

Overall, the EU's approach is more ambitious, proactive, comprehensive, and prescriptive compared to the US approach, and it is tough to compare these systems.

Navigating the Social Dilemma

The role of social media platforms has changed significantly since they first emerged. Platforms have become very powerful,[32] because of not just their increasing size or market power but also their access to all kinds of personal data[33] and their ability to apply algorithms and artificial intelligence to enhance users' experience—and increase their profits. As these technologies have developed, the platforms have gone from being relatively simple photo-sharing and messaging apps to having a more significant impact on society and the economy.

Reforms have not kept up with these digital platforms' tech development and increasingly powerful role.

For example, Facebook grew from an online photobook designed for Harvard students into a globally operating online social media and networking service that enables users to share content (including political information) and ads and reach the masses almost instantly. As a side effect of the popularity of online social networking, users (including decision makers and politicians) started using social media platforms for multiple purposes: for information and commerce but also political persuasion, even disinformation. Recently, Meta ended up intervening in a war between two sovereign nations, Ukraine and Russia. And besides "doing good" by blocking its users' geographical locations, it "does evil" when it facilitates incitement to violence against Russians on the platform.[34]

Reforms have not kept up with these digital platforms' tech development and increasingly powerful role. A static legal environment can have political consequences. For example, the Cambridge Analytica scandal and its continuing ripple effects,[35] leading up to the Mueller report on the alleged Russian interference with the 2016 presidential elections,[36] relit the spark of the "social dilemma."[37] This all shows the difficulties of how to tackle IT

regulation,[38] especially because different—seemingly concurrent—public interests are affected by tech regulation or nonregulation.

Although we can find some bad examples of using—and misusing—digital platforms, it is not necessary to draw rigid conclusions based on those. For instance, city transportation services should not be canceled because a few passengers cheat on purchasing tickets. There are alternatives to existing legal solutions to address new challenges.

In the case of platforms, decision makers should evaluate whether existing antitrust rules, contractual laws, and criminal laws can tackle the potential misuse of social media. It is probably unnecessary to control each segment of platform operation just to address security issues or avoid interventions in elections or wars. There is obviously no guarantee that social media platforms will operate "fairly" and in a nondiscriminatory way, though there is no evidence so far that algorithms are manipulating users or influencing their decisions illegally.

One must consider whether the platforms' potential opportunity to manipulate users is (in itself) enough to adopt a preventive regulatory framework. I do not intend to suggest that there are no valid concerns regarding the operation and influence of digital platforms or that there are no material breaches of laws when we consider the overall picture. There are. Nevertheless, there are some existing solutions to address data breaches and similar relevant crimes. If the existing rules prove to be ineffective, reforms should be carried out. However, presuming that those who have power will misuse it is questionable.

Communist regimes once stifled innovation and progress by requiring people, in effect, to "prove their innocence"—that is, to categorically prove, to the government's satisfaction, that an innovation was good and safe. It was disastrous, and in our time, it would be equally disastrous to regulate new technological innovation with a kind of "precautionary principle" that prohibits progress unless it can be proven completely safe and good, to the government's satisfaction. Such an approach stifles the marketplace for ideas and ultimately all the other marketplaces that benefit us too.

In the coming months and years, the US should not race to imitate Europe. At the very least, it should see how the European Union's detailed rules for the digital economy actually work out. By monitoring European reforms, the US can gain insight into how the market and consumers react and make informed decisions about which public interests to prioritize. The EU may be an early adopter of these regulations, but the US can still benefit by taking a more cautious approach and timing its decisions accordingly.

About the Author

Lilla Nóra Kiss is a visiting scholar and adjunct faculty at Antonin Scalia Law School at George Mason University and cofounder of the Freedom and Identity in Central Europe working group.

Notes

1. See Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford, UK: Oxford University Press, 2020).
2. Brett M. Pinkus, "The Limits of Free Speech in Social Media," *Constitutional Law* (Spring 2021), https://untdlaw.wixsite.com/accessible-law/post/the-limits-of-free-speech-in-social-media.
3. Ballotpedia, "Section 230 of the Communications Decency Act of 1996," https://ballotpedia.org/Section_230_of_the_Communications_Decency_Act_of_1996.
4. Lilla Nóra Kiss, "Monitoring Social Media," Law & Liberty, July 28, 2022, https://lawliberty.org/monitoring-social-media.
5. Bruce H. Kobayashi and Joshua D. Wright, "Antitrust and Ex-Ante Sector Regulaion," November 11, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3733740.
6. Adam Smith, *The Wealth of Nations* (London: W. Strahan and T. Cadell, 1776); and Joshua D. Wright and Jan M. Rybnicek, "A Time for Choosing: The Conservative Case Against Weaponizing Antitrust," *National Affairs* 54 (Winter 2023), https://nationalaffairs.com/time-choosing-conservative-case-against-weaponizing-antitrust.
7. US Department of Commerce, Bureau of Economic Analysis, "Digital Economy," January 12, 2023, https://www.bea.gov/data/special-topics/digital-economy.
8. Jan Eloff and Anna Granova, "Information Warfare," in *Computer and Information Security Handbook*, ed. John R. Vacca (Burlington, MA: Morgan Kaufmann, 2009), 677–90, https://www.sciencedirect.com/topics/computer-science/information-warfare.
9. US Department of Energy, "Cyber Security Is National Security," October 5, 2020, https://www.energy.gov/articles/cyber-security-national-security.
10. Bert Kondruss, "Worldwide Ransomware and Cyber Attacks January to June 2022," Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-2021-2.html; and Bert Kondruss, "IT Security: US Cyber Attack News," Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-usa.html#month2022-09.
11. Aela, "Unintended Consequences: The Unforeseen Impacts of Technology," September 19, 2022, https://aelaschool.com/en/strategy/unintended-consequences-the-unforeseen-impacts-of-technology.
12. Ben Smith, "How TikTok Reads Your Mind," *New York Times*, December 5, 2021, https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html.
13. White House, "Executive Order Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies," January 5, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-applications-software-developed-controlled-chinese-companies.
14. Katie Rogers and Cecilia Kang, "Biden Revokes and Replaces Trump Order That Banned TikTok," *New York Times*, June 9, 2021, https://www.nytimes.com/2021/06/09/us/politics/biden-tiktok-ban-trump.html; and Constitutional Discourse, "James C. Cooper–John M. Yun: Competing for or Against Privacy? On Using Competition Law to Address Privacy Issues," January 19, 2023, https://constitutionaldiscourse.com/james-c-cooper-john-m-yun-competing-for-or-against-privacy-on-using-competition-law-to-adress-privacy-issues.
15. Smith, "How TikTok Reads Your Mind."
16. Intersoft Consulting, "General Data Protection Regulation," https://gdpr-info.eu.
17. US Department of Commerce, International Trade Administration, "Privacy Shield Framework," https://www.privacyshield.gov/eu-us-framework.
18. Constitutional Discourse, "Márton Sulyok: 'How to Tackle IT?,'" March 8, 2021, https://constitutionaldiscourse.com/marton-sulyok-how-to-tackle-it.
19. Meta, "Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine," February 26, 2022, https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine; and Clare Duffy and Brian Fung, "Here's How Social Media Platforms

Are Responding to Russia's Invasion of Ukraine," CNN, February 26, 2022, https://www.cnn.com/2022/02/26/tech/social-media-response-russia-ukraine/index.html.

20. Isobel Asher Hamilton, "Meta Says It's Set Up a Special Team to Deal with Hate Speech and Misinformation Related to Ukraine," Insider, February 25, 2022, https://www.businessinsider.com/meta-ukraine-russia-invasion-special-operations-center-2022-2.
21. Isobel Asher Hamilton, "Facebook Says It Has a Special Team Taking Down Content Supporting or Praising the Taliban," Insider, August 17, 2021, https://www.businessinsider.com/facebook-says-it-has-special-team-taking-down-taliban-content-2021-8.
22. Sarah Al-Arshani, "Facebook Removed the Main Page of Myanmar Military as Protests Continue Following a Military Coup," Insider, February 21, 2021, https://www.businessinsider.com/facebook-removes-the-main-page-of-myanmar-military-2021-2.
23. Reuters, "Facebook Says It Did Not Do Enough to Halt the Spread of Hate Space and Violence in Myanmar," Insider, November 6, 2018, https://www.businessinsider.com/facebook-failures-in-myanmar-2018-11.
24. Constitutional Discourse, "Lilla Nóra Kiss: Professional Ethics and Morality Can Prevent Social Media from Becoming Sovereign," June 15, 2022, https://constitutionaldiscourse.com/lilla-nora-kiss-professional-ethics-and-morality-can-prevent-social-media-from-becoming-sovereign.
25. Adam J. White, "Google.gov," *New Atlantis*, Spring 2018, https://www.thenewatlantis.com/publications/googlegov. See also Google, "Google Receives $25 Million in Equity Funding," press release, June 7, 1999, https://googlepress.blogspot.com/1999/06/google-receives-25-million-in-equity.html.
26. Aela, "Unintended Consequences."
27. Bradford, *The Brussels Effect*.
28. Bradford, *The Brussels Effect*. See the book's description at Columbia Law School, "The Brussels Effect: How the European Union Rules the World," https://scholarship.law.columbia.edu/books/232.
29. European Parliament, "EU Digital Markets Act and Digital Services Act Explained," February 16, 2023, https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained.
30. European Commission, "The Digital Markets Act: Ensuring Fair and Open Digital Markets," https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.
31. Electronic Frontier Foundation, "DSA/DMA Adoption: Our Analysis," https://www.eff.org/pages/dsadma-adoption-our-analysis.
32. Constitutional Discourse, "Márton Sulyok: 'How to Tackle IT?'"
33. Constitutional Discourse, "Bianka Maksó: Lilla Nóra Kiss: Do Not Bury the Lede: Your Data, Their Money," April 1, 2022, https://constitutionaldiscourse.com/bianka-makso-lilla-nora-kissdo-not-bury-the-lede-your-data-their-money.
34. Marita Vlachou, "Meta Grants Exemption to Hate Speech Rules, Allowing Calls for Violence Against Putin," HuffPost, March 11, 2022, https://www.huffpost.com/entry/meta-facebook-hate-speech-russia-putin_n_622b2436e4b0317d0a2f1f11.
35. Shiona McCallum, "Meta Settles Cambridge Analytica Scandal Case for $725m," BBC, December 23, 2022, https://www.bbc.com/news/technology-64075067.
36. Roberst S. Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, US Department of Justice, March 2019, https://www.justice.gov/archives/sco/file/1373816/download.
37. Jeff Orlowski, *The Social Dilemma*, September 9, 2020, https://www.thesocialdilemma.com.
38. Constitutional Discourse, "Márton Sulyok: 'How to Tackle IT?'"

The project is generously supported by the John S. and James L. Knight Foundation.