

The Future of Speech Online: International Cooperation for a Free & Open Internet

Nick Clegg

This essay explores the impact that the resurgence of sovereignty has had on freedom of online speech. I argue that, in the past few decades, the internet has undergone a radical transformation from a universal tool of free communication to one that is increasingly fragmented into national and regional siloes. While acknowledging that recent internet regulation by democratic governments has been both necessary and inevitable, I argue that the authoritarian internet model – with citizens segregated from the rest of the global internet and subject to extensive surveillance and censorship – is on the rise, presenting a real risk to the internet as we know it. In the face of this threat, the world’s techno-democracies need to work together to protect the freedoms that the internet has so far made possible.

The internet is the latest in a long line of communications technologies to have enabled greater freedom of speech. From the printing press to the radio to the television and the cell phone, technological advances have made it possible for more people to express themselves, share news, and spread ideas. At every stage, speech has been further democratized, empowering people who could not previously make themselves heard and challenging the influence of the traditional gatekeepers of public information – including the state, the church, politicians, and the media. These advances have often been met first with excitement and enthusiasm, followed by a public backlash fueled by a mix of legitimate concerns about the impact of technology on society and moral panic stoked by the vested interests whose power has been challenged. In time, these pendulum swings have come to a resting point through a combination of the normalization of the technologies in society, the development of commonly understood norms and standards, and the imposition of guardrails through regulation.

The internet has enabled the most radical democratization of speech yet, making it possible for anyone with an internet connection and a phone or computer to express themselves, connect with people regardless of geographical barriers, organize around shared interests, and share their experiences across the world in

an instant. Over the last two decades, social media and instant messaging apps have turbocharged internet-enabled direct communication – and have exploded in popularity. More than one-third of the world’s population uses Facebook every day. More than one hundred forty billion messages are sent every day on Meta’s messaging apps, including Messenger, WhatsApp, and Instagram.

These technologies have made it possible for grassroots movements to grow rapidly and challenge established authority and orthodoxy, and in doing so, change the world – from the Arab Spring to the Black Lives Matter movement and #MeToo. A decade ago, sociologist Larry Diamond called social media a “liberation technology.”¹ Without the ability of ordinary people to share text, images, and video in close-to-real time, and to have it amplified via networks of people connected through social media apps like Facebook, Instagram, and Twitter, the groundswell of public support for these causes and others would never have been possible. Social media also made it possible for millions of spontaneous grassroots community-based initiatives to start and flourish during the emergency stages of the COVID-19 pandemic to help the vulnerable or celebrate frontline workers, and for millions of small businesses to stay afloat and reach customers during lockdowns.

It would be naive to assume that connection inevitably leads to progress or harmony. The free and open internet is not a panacea. With hindsight, the technoutopianism of the Arab Spring phase of social media was never going to last. But the pendulum has now swung far the other way, as it has done in the aftermath of previous technological advances, to a phase of techno-pessimism, with many critics decrying social media as the source of many of today’s societal ills. This backlash has led us to a pivotal moment for the internet. Politicians around the world are now responding to the clamor with a new wave of laws and regulations that will shape the internet for generations to come.

The radical liberalization of speech enabled by the internet brings its own set of issues and dilemmas: from what to do about the spread of misinformation, hate speech, and other forms of “bad” speech, to a range of novel issues around privacy, security, well-being, and more. These challenges are worthy of lengthy analysis and discussion in their own right – and they are the focus of other essays in this volume.

It is right that policymakers the world over are grappling with the many challenges the internet presents and beginning to establish a new generation of guardrails intended to mitigate the potential harms. But if we accept as our starting point that, for all the downsides, empowering people to express themselves directly is on the whole a positive thing for societies, and that this has been enabled by the open, borderless, and largely free-to-access internet, then we must not take it for granted.

In its early days, many thought that the internet’s distributed architecture and multi-stakeholder governance model would be enough to keep it open and free. It

was thought that the web was by design a technology that evades control by any single state or organization – an idea perhaps best captured in poet and political activist John Perry Barlow’s end-of-the-millennium manifesto, “A Declaration of the Independence of Cyberspace.”² As he rather grandly put it: “Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.” Alas, this idealism has proved to be misplaced. Events in recent years have demonstrated that the internet’s design is not enough to guarantee protection from government control.

The clash between borderless open communication and authoritarian top-down control is one of the greatest tensions in the modern internet age. Authoritarian and semi-authoritarian regimes have demonstrated over and over that when they want to quash dissent, one of the tools they use is the internet. They often try to do two things: 1) censor what their citizens can say, and 2) cut their citizens off from the rest of the global internet. And, as we have seen firsthand at Meta, to do these things they target the use of social media and messaging apps by their citizens.

The global open internet was built on democratic values – largely by American companies with American expectations of free expression, free enterprise, and freedom from government control. The collaborative, multi-stakeholder approach to the development of interoperable protocols and standards helped ensure that a piece of information could reliably be sent from one digital address to another using a single language known as the “Internet Protocol,” all without a government unilaterally deciding what those technical standards should be. That, in turn, laid the foundation for a boom in technological innovation, expression, and commerce that flowed over those networks in real time. For those of us living in Western democracies, this is likely the only model of the internet that we have ever experienced. But the global internet, in its truest sense, no longer exists. And what remains of it is being challenged by an alternative model.

The authoritarian internet model – with citizens segregated from the rest of the global internet and subject to extensive surveillance and censorship – is on the rise, presenting a real risk to the open, accessible internet as we know it. This is how China’s internet works today, and other countries have made similar moves to build digital walls – or entirely new networks – at their national boundaries. Russia, for example, was already moving this way before the internet clampdown that accompanied its invasion of Ukraine.

Artificial intelligence is the next frontier for freedom of speech online. AI is currently being developed by private companies, academic institutions, and governments – including authoritarian ones. Unlike the historical era in which the internet was developed – the 1990s and early 2000s – in which the liberal para-

digm of the internet was taken for granted, today we have competing visions that aim to shape the standards and norms of the next generation of transformative technologies.

The fracturing of the global internet into local and regional siloes is likely to intensify – by both accident and design – in the years ahead. As it does, it poses an ever-greater threat to free speech both online and offline. Writing new rules for the internet has increasingly become an opportunity for governments to pursue their economic and social agendas, as well as the stuff of manifestos, sloganeering, and geopolitical horse-trading. As tech issues have risen in political salience, populist nationalism has found expression in the debate about the internet.

This new digital nationalism is not solely the preserve of authoritarian states. As is the case with the wider rise of populist nationalism globally, elements of digital nationalism are also creeping into the debate in open democratic societies. For example, talk of “digital sovereignty” and “data localization” – asserting a nation’s right to stop or limit the free flow of data across borders – is now commonplace. These ideas increasingly underpin new laws. As they do, they chip away at the foundations of the open internet, which relies on cross-border data flows, and play into the hands of authoritarian regimes who see these terms being used in places like the EU and use it as political cover for their own more onerous restrictions.

Of course, it’s right that governments should seek to express national sovereignty over matters of national importance to them. Barlow’s declaration of independence from government control came when the internet was still nascent with a fraction of the billions of people who are online today. Ultimately, the phase of global internet regulation happening right now is necessary given the internet’s level of maturity and its scale of impact on society, and many new internet regulations are designed to actively protect freedom of speech online. But the broader rise of digital nationalism poses an existential threat to the open internet, and in particular, the profoundly liberating effect it has had on people’s ability to express themselves freely.

In a number of regions around the world, we have seen attempts by governments to silence citizens, control the flow of information, and manipulate public debate. This is increasingly the case during times of war and social unrest, when apps like Facebook, Instagram, Twitter/X, TikTok, YouTube, WhatsApp, and Messenger are used by ordinary people to connect within and across borders to make their voices heard, to share news and information, and to organize and rally support. Nowhere has this been more apparent in recent years than in Russia’s invasion of Ukraine and during recent mass protests in Iran.³

Within days of Vladimir Putin’s full-scale invasion of Ukraine, Russia attempted to block or restrict access to Facebook and Instagram as part of a wider attempt to cut Russian citizens off from the open internet, silence people and independent media, and manipulate public opinion. State-controlled media outlets and Russia-

based covert influence campaigns also kicked into gear to spread propaganda and misinformation and to subvert media narratives beyond its borders. In recent years, Meta and others have become increasingly savvy about how to identify and take down these campaigns, not just on their own platforms but across the internet through cross-industry cooperation. Since 2017, Meta has disrupted more than two hundred so-called “coordinated inauthentic behavior” networks globally.⁴

The widespread protests in Iran that began in the wake of the awful killing of Jîna Emînî, a Kurdish woman better known as Mahsa Amini, led to the Iranian government clamping down aggressively on speech and freedom of assembly, as well as limiting the use of the internet and apps like Instagram.⁵ It’s little wonder why: Instagram has been widely used by Iranians to shed light on the protests and the brutal response of the regime. Since Emînî’s death, hashtags related to the protests in Iran have been used on Instagram more than one hundred sixty million times. #MahsaAmini was the fifth top hashtag globally during the first three months of protests, demonstrating the power of social media to help create awareness in these critical moments. Protestors also shared Instagram footage of the protests with international media outlets, many of whom couldn’t report directly from Iran.

Clampdowns by authoritarian regimes on the use of social media and the wider internet are not limited to times of acute crisis. Increasingly, they are also using content and data laws to suppress free speech.

Laws that seek to come to grips with the proliferation of content online do not inherently have to impinge on the right of citizens to express themselves freely. Perhaps the best example of internet legislation that actively protected free speech comes from a generation ago. The last time the United States enacted significant internet regulation was 1996, when Section 230 of the Communications Act was created to address liability for online content.⁶ The statute protects free speech by making online services immune from civil liability for the actions of their users while providing protections for platforms to moderate content. This combination of simple tools – a shield from liability for hosting speech generated by others, and the latitude to moderate that content – has often been hailed as an integral enabler of speech in the digital era that also unlocked innovation and commerce. But it is hard to imagine such a law being passed in today’s climate. And Section 230 itself has not been preserved in aspic since the 1990s. For example, in 2018, the Fight Online Sex Trafficking Act / Stop Enabling Sex Traffickers Act was passed to clarify that Section 230’s liability protections did not mean exemption from enforcement of federal or state sex trafficking laws.⁷

Of course, technological capabilities have also evolved exponentially in the last quarter-century, which is why updating Section 230 has been fiercely debated in

Washington and elsewhere in recent years. Done well, Section 230 reform can continue to promote free speech while equipping companies with the tools to combat harmful content such as child exploitation, pornography, incitement of violence, and bullying and harassment. Meta has spoken out in support of updating Section 230 to require platforms to be more transparent about their standards, processes, and actions; establish regular reporting requirements; and maintain a safe harbor approach, in which larger platforms are required to demonstrate that they have robust practices for identifying illegal content and quickly removing it. Any such requirements, Meta has argued, should not adversely affect the playing field for nascent or smaller companies that have less capacity to comply with a complex regulatory regime, with exemptions or modifications for those entities as needed.

Of course, cultural attitudes and historical sensitivities vary widely around the world, and nation-states have a sovereign right to determine what is legal and illegal speech in their territories. Doing so by no means represents a mortal threat to free expression. Few would argue, for example, that Germany's ban on Holocaust denial is unreasonable.

The threat to free speech comes from laws designed to quash dissent, restrict political speech, or otherwise infringe international human rights norms. China's restrictive "Great Firewall of China" content laws are well-known: there are vast swathes of websites that Chinese users are blocked from accessing, while news, satire, and other content are frequently censored.⁸ And these restrictions can have knock-on effects beyond China's borders. Chinese-owned TikTok is one of the fastest growing social media apps in the world, but has been accused of restricting political content globally, including videos of prodemocracy protests in Hong Kong.⁹

Individual companies will decide for themselves when to stand firm and when to acquiesce in the face of laws or government requests they disagree with, but not without consequences. Companies like Meta receive countless requests from authorities in countries democratic, authoritarian, and in-between to remove political content, often accompanied by threats of fines if they fail to comply, and often shrouded in vague justifications of maintaining national security or public order. In some cases, refusal to remove content can lead to access to these platforms being throttled (a means of intentionally slowing internet traffic to a halt). And laws have been proposed in some countries requiring internet companies to designate local employees who can be held responsible by local law enforcement, adding an unsettlingly personal element to any refusal to cooperate with government requests.

Of course, if resisting attempts by authorities to censor content on a company's platform comes at too high a price, the alternative is to withdraw services from that market altogether. In either case, free speech is restricted. Either citizens use a platform that limits their ability to express themselves, or they lose the ability to use the platform to express themselves at all. But while censorship poses a direct threat to free speech online, another characteristic of digital nationalism – the

desire to limit the flow of data across national borders – poses an indirect but no less significant one.

For all intents and purposes, China’s internet is separate from the rest of the global internet. Not only does China’s internet model impose restrictions on content, it also requires restrictions on the flow of data in and out of the country, essentially creating a digital wall at its national border. As digital nationalism takes hold in other countries, support for data localization has grown.

For some policymakers, the motivation behind data localization policies is economic – albeit based on a deeply flawed misconception that “data is the new oil” – a scarce resource to be hoarded, enriching those who own the most. As I have argued elsewhere, notwithstanding the fact that it is a valuable resource for those who know how to obtain relevant insights from it, data is a nonrivalrous good rather than a finite commodity to be owned and traded, pumped from the ground and burned in cars and factories.¹⁰ As such, the value of data does not lie in hoarding it, but in the network effects produced by global flows of data. It is this freedom of information flows that makes the internet, and its underlying structure of data, valuable not just for companies like Meta, but for billions of individual users, small businesses, civil society organizations, and researchers across the world. Fixating on where data is stored and processed is a red herring; its value can be derived regardless of where it is stored globally.

Nonetheless, this idea has influenced policymakers in a number of countries, and not just where authoritarian regimes are in power. While “hard” data localization policies result in an almost complete enclosure of a country’s data economy within national boundaries, the desire to impose greater national sovereignty over data has increased support for “soft” data localization policies in many open democracies. This milder form of localization requires data to be mirrored in local servers, so that copies are held domestically, which has the effect of slowing internet services and limiting access to them. Indeed, support for data localization in liberal democracies unwittingly gives legitimacy to the actions of authoritarian governments who want to impose harsher control over the internet.

Following this trend, governments around the world are growing more aggressive in their demands for private platforms to comply with rules to produce data, block content, and break the end-to-end encryption that keeps messaging services private and secure. What’s more, as the Center for Strategic and International Studies put it:

National security justifications for these mandates are often thinly veiled attempts at asserting greater control of the domestic digital domain; meanwhile, data localization has had negative impacts on human rights, privacy, and economic interests.¹¹

These developments create the conditions for the splintering of the open internet, with all the negative impact that this will have for freedom of speech around the world. This splintering not only risks changing the character of the existing internet, but also threatens to shape the next generation of transformative technologies powered by artificial intelligence – from “generative AI” tools that use machine learning systems to create new text and visual content, to “metaverse” technologies like virtual reality, augmented reality, and mixed reality that could reshape the way we work, learn, and play.

Without global cooperation on the development of the standards underpinning these powerful new technologies, they could be fragmented from the start. Instead of universal standards, we will have an arms race between different models, underpinned by different values, leading to a more technologically, socially, and culturally divided world than ever before.

We need a counterweight to the spread of the authoritarian internet. The world’s techno-democracies must recognize and actively promote and defend the idea of the open internet. The announcement of an agreement to protect open data flows between the United States and the European Union is a necessary step, as are the principles enshrined in the “Declaration for the Future of the Internet” announced by the Biden administration and signed by dozens of governments in 2021.¹² We need concrete actions to follow.

To protect against the spread of the authoritarian internet, the democratic world needs a shared sense of ambition and urgency. In 1944, with the end of World War II in sight, the Allies gathered in Bretton Woods, New Hampshire. After a month of intense negotiations, an agreement was struck that became the foundation of global stability in the postwar era. Bretton Woods led to a new global governance philosophy based on the idea that if nations large and small ceded a degree of their own sovereignty to abide by the same global rules, it would prevent a return to the protectionism and economic catastrophes of the 1920s and 1930s. Global institutions like the International Monetary Fund (IMF) and the World Bank were created to promote economic growth and political stability for all. We need that same scale of ambition to unite the democratic world today. The internet has been one of the great collective achievements of humanity. It is time for its Bretton Woods moment. A shared sense of purpose based on universal values like free expression, transparency, and accountability could be the foundation for an international consensus that governments, industry, and civil society can organize around.

If we want to create a system with the teeth necessary to rigorously defend the open internet, we need an international body with the ability to hear complaints and adjudicate them when conflicts of law arise. This mechanism could apply to conflicts related to laws that impede data flows or undermine the protocols on which network interoperability relies, but also to resolving jurisdiction questions

related to other conflicts of law. States that signed up to such a body would be bound by its decisions, and expected to uphold shared values and refrain from regulating the internet in ways that put other countries at a disadvantage.

However, given the growing geopolitical chasm between the United States and the European Union on one side and China and Russia on the other, it may be wishful thinking to imagine the creation of meaningful new multilateral global institutions – the Bretton Woods moment and postwar institutions were made possible by the destruction of the Axis powers, and no such total victory over authoritarian control of the internet is possible. Therefore, an incremental approach is more realistic. Policy scholars Tanya Filer and Antonio Weiss have argued that the future of international cooperation lies in “digital minilaterals,” which they describe as “a small, trust-based network with a shared set of values oriented around innovation and the creation and sharing of knowledge.”¹³

Starting small is key to redeveloping the kernels of trust that have been lost in this climate of rising nationalism. Alongside the IMF and World Bank, an “International Trade Organization” was originally envisaged as part of the postwar Bretton Woods system as a necessary bulwark against the protectionist policies that contributed to the outbreak of war. Instead, the international community chose to enact a series of rules under the General Agreement on Tariffs and Trade (GATT), before finally setting up the World Trade Organization (WTO) to oversee those rules in 1995. A similar trajectory could be necessary for the sort of international cooperation required today to eventually blossom.

Indeed, the WTO could provide a forum for democracies to come together around a GATT-style arrangement on international data flows and other digital issues. It could include just a few key players at first, with the intention of expanding over time. Such an approach goes with the grain of recent attempts to get multinational agreement on digital issues. For example, leading WTO countries have taken steps toward a new global trade agreement on cross-border e-commerce. The 2019 plurilateral joint statement on e-commerce has now been signed by scores of WTO countries.¹⁴ The statement includes the United States and China, but not India. Persuading India and others to join the e-commerce negotiations should be an integral part of the future of this process. The United States, European Union, and their allies could pursue a coordinated effort that would tie joining the e-commerce agreement with economic and political incentives. This could take the form of economic assistance, direct investment, and political support in international fora where appropriate.

The WTO could also bring democracies to the table around other pressing challenges, like regulatory coordination and expanding the CLOUD Act – which enables data to be shared for investigations of serious crime – to include more countries beyond the United States, the United Kingdom, and Australia. As the U.S. Department of Justice proudly proclaimed, the CLOUD Act “represents a

new paradigm: an efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data.”¹⁵ This new paradigm should reach more democracies.

This approach – using the WTO to bring key democracies together around agreements that then expand to include more countries – could be a great starting point for global alignment on AI regulation, too. The Biden administration has already signaled its intention to legislate to safeguard privacy and civil rights in the use of AI technologies.¹⁶ Using its global clout to bring nations together to establish common standards around AI would help to ensure democratic values are baked in as these technologies are developed across the democratic world.

Whatever the forum, democracies need to do more to provide support and guidance to private platforms in protecting free speech and defending human rights when they operate in authoritarian and semi-authoritarian countries. Starting small to get agreement between key players may be necessary, but the ambition should be global. Multi-stakeholder institutions in particular – in which government, industry, civil society, academia, and technical experts come together on equal footing – can support the development of a framework of actions that private platforms can take to do this across the globe and provide guidelines for the kinds of speech that need to be protected.

We are living through an extraordinary period. In three decades, the internet has radically democratized speech and transformed the global economy. And a new generation of technologies – from hugely powerful AI systems to metaverse technologies like virtual and augmented reality – promise to deepen the integration of data-driven technologies in every corner of our societies. Necessary new waves of laws to govern digital technologies are being written in capitals around the world, and governments are becoming increasingly savvy and sophisticated in how they harness technological progress to their domestic and global advantage.

The result is that the internet is changing – but not necessarily for the better. After a period of extraordinary openness, the internet is increasingly being carved up into national and regional silos. With each new national restriction, the internet becomes a little less free, and the digital economy becomes a bit more constrained. Slowly, the authoritarian internet replaces the open internet, and authoritarian values replace democratic ones online, not the least of which is the belief in free expression.

In the face of this threat, democracies have a responsibility and a choice: actively support the open internet or stand by silently as digital nationalism reshapes it piece by piece. Defending the open internet is still possible, but it will require serious political will and leadership, particularly from the world’s leading techno-democracies such as the United States, European Union, India, and other significant leaders in this field like Japan, Australia, and South Korea. They not only need to reject digital nationalist policies domestically, but to cooperate to

guard against them internationally. We cannot afford any more benign neglect. The internet requires not a more intense version of digital nationalism, but rather a renewed belief in international and regional collaboration that aims to protect the freedoms that the internet has so far made possible to all.

ABOUT THE AUTHOR

Nick Clegg is President of Global Affairs at Meta. He served in the UK Parliament from 2005 to 2017, where he became leader of the Liberal Democrat party in 2007 and served as Deputy Prime Minister in the UK's first coalition government since the war, from 2010 to 2015. He also served as a member of the European Parliament from 2000 to 2005. He was appointed a Knight Bachelor in 2018. He is the author of *Politics: Between the Extremes* (2016) and *How to Stop Brexit (and Make Britain Great Again)* (2017).

ENDNOTES

- ¹ Larry Diamond, "Liberation Technology," in *Liberation Technology: Social Media and the Struggle for Democracy*, ed. Larry Diamond and Marc F. Plattner (Baltimore: Johns Hopkins University Press, 2012), 3.
- ² John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, <https://www.eff.org/cyberspace-independence> (accessed August 23, 2023).
- ³ Raksha Kumar, "Not Quite the Arab Spring: How Protestors Are Using Social Media in Innovative Ways," Oxford University Reuters Institution, December 6, 2022, <https://reutersinstitute.politics.ox.ac.uk/news/not-quite-arab-spring-how-protestors-are-using-social-media-innovative-ways>.
- ⁴ For more information, see "Security at Meta," Meta, <https://transparency.fb.com/meta-security> (August 22, 2023).
- ⁵ Akash Sriram, "As Unrest Grows, Iran Restricts Access to Instagram, WhatsApp," Reuters, September 21, 2022, <https://www.reuters.com/world/middle-east/iran-restricts-access-instagram-netblocks-2022-09-21>. For more information on Jîna Emîni's name, as well as Masha Amini, the Arabic name that the Islamic Republic (IR) forced her to use (the IR neither recognizes nor allows the Kurdish language in any official documents), see Azadeh Shahshahani and Yosi Badie, "Iran's Brutal Crackdown on 'Women, Life, Freedom,'" *The Nation*, September 28, 2022, <https://www.thenation.com/article/world/iran-protests-jina-emini>.
- ⁶ 47 U.S.C. § 230.
- ⁷ Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-165, 132 Stat. 1253.

- ⁸ Yaqiu Wang, “In China, the ‘Great Firewall’ Is Changing a Generation,” *Politico*, September 1, 2020, <https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385>.
- ⁹ Alex Hern, “Revealed: How TikTok Censors Videos That Do Not Please Beijing,” *The Guardian*, September 25, 2019, <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing>.
- ¹⁰ Nick Clegg, “Data: What It Is, What It Isn’t, and How Misunderstanding It Is Fracturing the Internet,” *Medium*, September 20, 2022, <https://nickclegg.medium.com/data-what-it-is-what-it-isnt-and-how-misunderstanding-it-is-fracturing-the-internet-e56e278643a7>.
- ¹¹ Erol Yayboke, Carolina G. Ramos, and Lindsey R. Sheppard, “The Real National Security Concerns over Data Localization,” *Center for Strategic and International Studies*, July 23, 2021, <https://www.csis.org/analysis/real-national-security-concerns-over-data-localization>.
- ¹² “FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework,” *The White House*, March 25, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework>; and “FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet,” *The White House*, April 28, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet>.
- ¹³ Tanya Filer and Antonio Weiss, “Digital Minilaterals Are the Future of International Cooperation,” *Brookings Institution*, October 16, 2020, <https://www.brookings.edu/articles/digital-minilaterals-are-the-future-of-international-cooperation>.
- ¹⁴ “Joint Initiative on E-commerce,” *World Trade Organization*, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm#how (accessed August 22, 2023).
- ¹⁵ Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, U.S. Department of Justice, April 2019, <https://www.justice.gov/opa/press-release/file/1153446/download>.
- ¹⁶ Garance Burke, “White House Unveils Artificial Intelligence ‘Bill of Rights,’” *Associated Press*, October 5, 2022, <https://apnews.com/article/technology-business-artificial-intelligence-7a39848340d210592aeea2478225f489>.