NEW AMERICA

October 2023

Governing the Digital Future

Gordon LaForge & Patricia Gruver

Planetary Politics

Last edited on October 02, 2023 at 9:16 a.m. EDT

Acknowledgments

The authors would like to thank Candace Rondeaux, Senior Director of New America's Planetary Politics initiative, for invaluable guidance conceptualizing and steering the production of this report and the research that informed it. Planetary Politics Director Heela Rasool-Ayub provided helpful editorial direction. Several colleagues at New America contributed time, effort, and thought to this project, notably Public Interest Technology Senior Program Manager Alberto Rodriguez, Open Technology Institute Senior Policy Analyst David Morar, Future Frontlines Program Manager Ben Dalton, and Digital Impacts and Governance Initiative Senior Advisor Allison Price.

We are grateful also to the dozens of collaborators who contributed to the research process and who are too numerous to list in full here. Deborah Avant of the University of Denver's Sié Center, Tithi Chattopadhyay at Princeton University's Center for Information Technology Policy, and Shawn Walker and Michael Simeone at Arizona State University helped plan and carry out the research agenda. We are indebted to the Digital Futures Task Force, especially working group leads Constanza Gomez-Mont, Alejandro Pisanty, Sagwadi Mabunda, Swati Srivastava, Landry Signe, and Robin Renee-Sanders. A crack team of rapporteurs, including Merle Weidt, Kenia Hale, Jonas Heering, Abigail Giles, and Summer Boucher-Robinson, captured and distilled a staggering amount of information. Early internet luminaries Vint Cerf, Mike Roberts, and Roberto Gaetano generously gave their time to share an under-the-hood look at ICANN.

Gratitude is also due to New America intern T Nang Seng Pan, who diligently fact-checked the report and created compelling and informative visualizations with the assistance of Naomi Morduch Toubman. Sabrina Detlef performed sharp copyedits, and Kelley Gardner managed the layout. Melissa Salyk-Virk provided indispensable organizational support throughout the research process. This project was made possible by a grant from the Ford Foundation, where Salih Booker and Alberto Cerda Silva were integral thought partners whose insights helped shape the research and report.

Editorial disclosure: The views expressed in this report are solely those of the authors and do not reflect the views of New America, its staff, fellows, funders, or its board of directors.

About the Author(s)

Gordon LaForge is a senior policy analyst at New America working on global politics.

Patricia Gruver is an international tech policy expert, with expertise in tech diplomacy.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Planetary Politics

New America's Planetary Politics initiative is a call to action for reimagining a more inclusive, equitable, and sustainable global order. As our world becomes hotter, wetter, and more complex, the time to build new global institutions attuned to today's environment—in preparation for tomorrow—is now.

Contents

Contents Cont'd

At a Glance

- Worsening power asymmetries are at the heart of much conflict, harm, and governance dysfunction in the digital domain.

- Power in and over the digital realm is more concentrated than ever before, as outsized corporate influence and increasing government control create a trajectory for the digital future that imperils security, equity, and human rights.

- At the same time, the digital domain is the most active battlefield in an escalating, zero-sum power struggle between the U.S. and China, and intensifying skirmishes between established and emergent leaders in digital tech such as Russia and India.

- Countering global power imbalances and promoting an equitable, safe digital domain will take an intentional approach to expanding the multi-stakeholder global governance ecosystem.

- We have an opportunity to get in front of some of the worst possible harms stemming from artificial intelligence right now. To do that, we will need to invest in institutional vehicles committed to paying it forward to future generations when it comes to ensuring a safe, secure, and equitable digital domain.

- Stewardship of connectivity needs to shift away from internet service providers and corporate power toward a more distributed model based on various fail-safes so as to enable alternative and redundant means of access.

- In the contest to shape global standards in areas like cybercrime, privileging regional guidelines could prove more fruitful than the pursuit of universal requirements.

- To reduce global conflict and harm from digital surveillance, democracies should practice what they preach and ban commercial spyware outright.

- The big data value chain must be reformed to afford individuals and less influential countries more rights and proceeds from their data.

Executive Summary

The digital world is in disarray. For all their benefits, digital technologies have unleashed harms ranging from algorithmic bias and disinformation to ransomware attacks. Rising inequality, social and political divisions, and escalating geopolitical tensions have darkened more hopeful visions of our shared digital future. Tech companies, arguably the most powerful private entities in history, are racing to deploy powerful artificial intelligence (AI) systems that will transform societies. At a time when global cooperation is essential, governance is fragmented within the different layers of the digital domain and failing to manage risk and conflict. Never before has the future of the digital revolution felt so uncertain and contested.

By now, the ills of digitization are well-trod research terrain. Yet, there are poorly understood divergences in how different nations, sectors, epistemic communities, and socioeconomic groups perceive, experience, and address digital harm. From January through June 2023, New America's Planetary Politics initiative undertook a research agenda to understand these fault lines and to identify first-order principles that could move the digital world toward greater safety and equity. To do this, we conducted an extensive literature review, consulted with experts and hosted workshops, and convened a global, multidisciplinary group of researchers, technologists, and policymakers we named the Digital Futures Task Force.

The first part of this analysis was focused on **five issue areas** in digital technology that are driving conflict, human rights violations, and socioeconomic displacement: **(1) AI and algorithmic decision-making, (2) digital access and divides, (3) data protection and data sovereignty, (4) digital identity and surveillance, and (5) transnational cybercrime.**

We then mapped the where, why, and how of the ways competition, contestation, and cooperation in those five issue areas are shaping the patchy global digital governance landscape today. What came through right up front was that trend-setting nation-states including the United States, China, European Union, and India have divergent visions for the digital future. Arguably, Russia, too, falls within this category of trendsetters as well but more as a result of its default to adopting policies, customs, and approaches to tech governance that fall in line with China's vision. Now more than ever, we see the ways clashes between those trend-setting states are spilling into the open in multilateral fora focused on shaping global cyber norms. Large American technology companies are digital sovereigns in their own right, with governing power to rival that of governments. Amid increasing contestation, multi-stakeholder institutions still find consensus among diverse interests to manage the global internet.

From our dialogues, consultations, and analysis, a fundamental conclusion emerged: An over-concentration of power and severe power asymmetries are causing conflict, harm, and governance dysfunction in the digital domain. Whereas the internet began as a distributed enterprise that connected and empowered individuals worldwide, extreme concentrations of political, economic, and social power now characterize the digital domain. Power imbalances are especially acute between developing and wealthy nations, as a handful of rich-world tech companies and nation-states control the terms and trajectory of digitization.

The Digital Futures Task Force identified first principles for positive interventions and explored governing frameworks for countering power asymmetries and steering the world toward a safer, more equitable digital future. At a conceptual level, this will take not a single international agency, but rather a networked, multi-stakeholder ecosystem of institutions, agreements, and initiatives that work as a fluid, shifting, federated whole, like, in the words of one task force member, a school of fish moving individually yet in concert through a changing current.

On a more practical level, a few takeaways and first principles stood out as in need of urgent attention:

1. We have a critical opportunity to get ahead of possible harms that will stem from AI; science and citizen-centric fora like the Pugwash Conferences on Science and Technology offer a model means of refocusing the digital governance ecosystem beyond the myopic logic of national sovereignty.

2. Amid digital divides and increasing government control over the internet, multilateral and multi-stakeholder agencies should invest in fail-safes, alternative or redundant means of access, that can shift the stewardship of connectivity away from concentrated power centers.

3. Regional standards that respect diverse local circumstances can help generate global cooperation on challenges such as cybercrime.

4. To reduce global conflict in digital surveillance, democracies should practice what they preach and ban commercial spyware outright.

5. Redistributing the value from big data can diminish corporate power and empower individuals.

From a research perspective, more work is needed to understand and draw attention to the ways digital power asymmetries between the rich and developing worlds are shaping opportunity, risk, and sovereignty. In the next year, we plan to

reconvene an expanded Digital Futures Task Force to conduct further analysis in two areas: (1) AI governance and impacts in the developing world and (2) the battles over digital sovereignty playing out in Africa, Latin America, Southeast Asia, and the Middle East.

We intend this report and the next phase of work as a modest contribution to the effort to bring about principled stewardship of the digital domain. We believe more global engagement and attention to power imbalances are essential to address the widening gaps among nations and resolve conflicts between corporations, governments, and citizens over the contours of sovereignty in the digital domain.

Introduction

As we enter the age of AI, the digital future appears uncertain. Even before the advent of large language models, digital technologies were straining and fracturing economic, political, and social systems. From Myanmar to the United States, algorithmically boosted hate and disinformation fuel polarization and political violence. Digital state surveillance violates human rights, while corporate surveillance deprives citizens of value and dignity and drives addictive social media platforms that many think are precipitating a mental health crisis among teenagers and young adults.[1] Cybercrime causes billions of dollars in losses to governments and companies and threatens critical infrastructure. The open, global internet is in peril, as governments more frequently shut down access and seek to steer cyber norms toward authoritarian frameworks. Control of data, network infrastructure, semiconductors, and governance of the internet itself is at the heart of escalating geopolitical competition, particularly between the U.S. and China.

It will take governance systems to mitigate the risks and harms of the digital revolution. Yet so far, global digital governance is incoherent and patchwork—fractured along technical, national, geographic, and sectoral lines. Countries impose domestic regulations, but cyberspace is transnational, and digital technologies proliferate at astonishing speed. These technologies challenge the centuries-old notion of sovereignty as distinctly territory-bound, a consensus that has underpinned the international order for centuries. The sovereignty of nation-states still depends on control over physical terrain, but in the theoretically borderless landscape of cyberspace, sovereignty is unbound from conventional geography.

Geopolitical competition, divergent national visions of digital sovereignty and governance, and the power of the private sector mean nation-states struggle to agree on norms to sustain an equitable, safe, and innovative digital domain. The consequential, and in some cases widening, divides between developing and wealthy nations over priorities, impacts, perspectives, and resources illustrate the need not so much for consensus as for justice. Effective global digital governance will depend not on imposing conformity or aligning ideologies, but on developing frameworks and institutions that can rectify power imbalances, as well as make space for areas of agreement and cooperation.

"Effective global digital governance will depend not on imposing conformity or aligning ideologies, but on developing frameworks and institutions that can rectify power imbalances, as well as make space for areas of agreement and cooperation."

The scale and complexity of the digital domain makes global governance all the more difficult. Consider, for example, the current dynamics of global cooperation and competition in each of the internet's four layers. The physical layer features intensifying competition between the U.S. and China to control network architecture and infrastructure, such as subsea cables and semiconductors.[2] The logic layer, the "central nervous system of cyberspace," functions coherently under the supervision of multi-stakeholder bodies like the Internet Corporation for Assigned Names and Numbers (ICANN), but autocratic countries are trying to bring this layer under greater state control, which threatens to splinter the global internet.[3] The platform or application layer is highly fragmented, with different nations adopting different regulatory frameworks and Silicon Valley corporations in the United States wielding more governance power than all but a handful of nations. The machine layer, where powerful AI systems are emerging, is the focus of many regulatory proposals, yet risks defaulting to the same shambolic governance dynamics of the platform layer.

With these challenges and issues in mind, New America's Planetary Politics initiative spent six months examining fault lines in the digital domain and the gaps and prospects for global digital governance. We started with an examination of digital harm worldwide. There are a variety of reasons to start with harms when thinking about the governance of an emerging technology. For one, it is generally easier to find agreement around the question of what is harmful rather than the question of what is good, as humans are wired to be risk-averse, overweighting the impact of potential negative outcomes relative to potential gains.[4] The legal and ethical codes of societies tend to focus on deterring what is bad rather than encouraging what is good.

We focused on five issue areas that are generating risk and harm for societies everywhere:

1. AI and algorithms;

2. Digital access and divides;

3. Data protection and data sovereignty;

4. Digital identity and digital surveillance; and

5. Transnational cybercrime.

We conducted a literature review to understand the tensions and areas of contestation in the academic, policy, and public debates surrounding these issues. Then, to deepen and broaden the inquiry, we convened groups of experts and practitioners. The first forum was a workshop featuring scholars and civil society leaders who either study, manage, or are otherwise involved in initiatives that attempt to exercise democratic governance over aspects of the digital domain (e.g., the Facebook Oversight Board, the Global Network Initiative, the Digital Trust and Safety Partnership). A series of virtual consultations followed, including one with former leaders of ICANN, the multi-stakeholder body that manages the Domain Name System (DNS), the phonebook of the indexed internet.

The culmination of this effort was the establishment of the 30-member Digital Futures Task Force, the first step on a multiyear process that New America has undertaken to shape the public debate on preventing, mitigating, and managing digital harms. The task force consists of five working groups, one for each issue area. Each working group had six members, each either hailing from or focused in their work on a different region: Africa, Latin America, North America, Europe, the Middle East, and Asia. We anticipate that membership will continue to grow as we take aim at making the debate about the digital future more inclusive and equitable.

The geographical range aimed to bring developing and wealthy nations' perspectives in equal weight. Task force members include distinguished scholars and researchers, diplomats, law enforcement officials, technologists, entrepreneurs, and lawyers. The essential selection criteria was diversity—of nationality, identity, expertise, and experience. In May, the task force convened for a two-day symposium in Washington, DC, in which the working groups mapped harms and areas of contestation in their issue area and began pointing the way to principles and frameworks for governance.

We had three questions to answer.

First, we sought to identify some of the global fault lines that are shaping the digital future: Where and how do scholars, policymakers, cultures, sectors, and socioeconomic groups diverge in their experience and perception of digital harm and risks? **Second,** we wanted to map the existing global digital governance landscape: Which nations, companies, multilateral organizations, and multi-stakeholder bodies are shaping the digital domain, and how? **Lastly,** we wanted to identify potential solutions: What new governing frameworks and institutional models could bring greater security, equity, and prosperity to the digital future?

Digital Fault Lines

AI and Algorithmic Decision-Making

First coined in the 1950s by American computer scientist John McCarthy, the term *artificial intelligence* refers to machines that can learn and make decisions or predictions in ways that simulate or mimic human intelligence.[5] Scholars treat AI as an umbrella concept that encompasses a range of both current and potential future technologies. They credit this flexibility for enabling continuity even as the technology and its uses have changed, but the lack of a precise definition has confounded alignment among legislative and regulatory processes and has invited litigation.[6]

In policy debates, the most salient branch of AI is machine learning, whereby algorithms trained on datasets to detect patterns and make inferences are able to describe something, predict what will happen, or prescribe what action to take. Machine learning has advanced at an astonishing pace in recent years, owing to falling costs of computation, the availability of massive amounts of data, and the development of more sophisticated algorithmic models.[7] Machine learning is now commonplace, at use around the world in sectors including health care, entertainment, manufacturing, policing, and national security. These systems have unlocked greater efficiencies, generating billions in revenue, and helping solve public policy problems, such as social assistance targeting.[8]

They also carry risks and harms. Ill-designed or insufficiently trained systems have caused physical injury and even death, such as in the case of vehicle crashes caused by autonomous self-driving systems.[9] The massive quantities of data collected to train AI systems raise concerns for privacy, as researchers argue that the established privacy discourse—which relies on the assumption that data is a tradable good over which its creator has agency—is moot when a system's operations are so complex that they cannot be understood, a growing power asymmetry present in AI systems.[10] Extensive literature has illustrated the propensity for opaque, algorithm-based machine learning systems to exhibit bias and discriminate based on race, gender, or other socioeconomic qualifiers.[11]

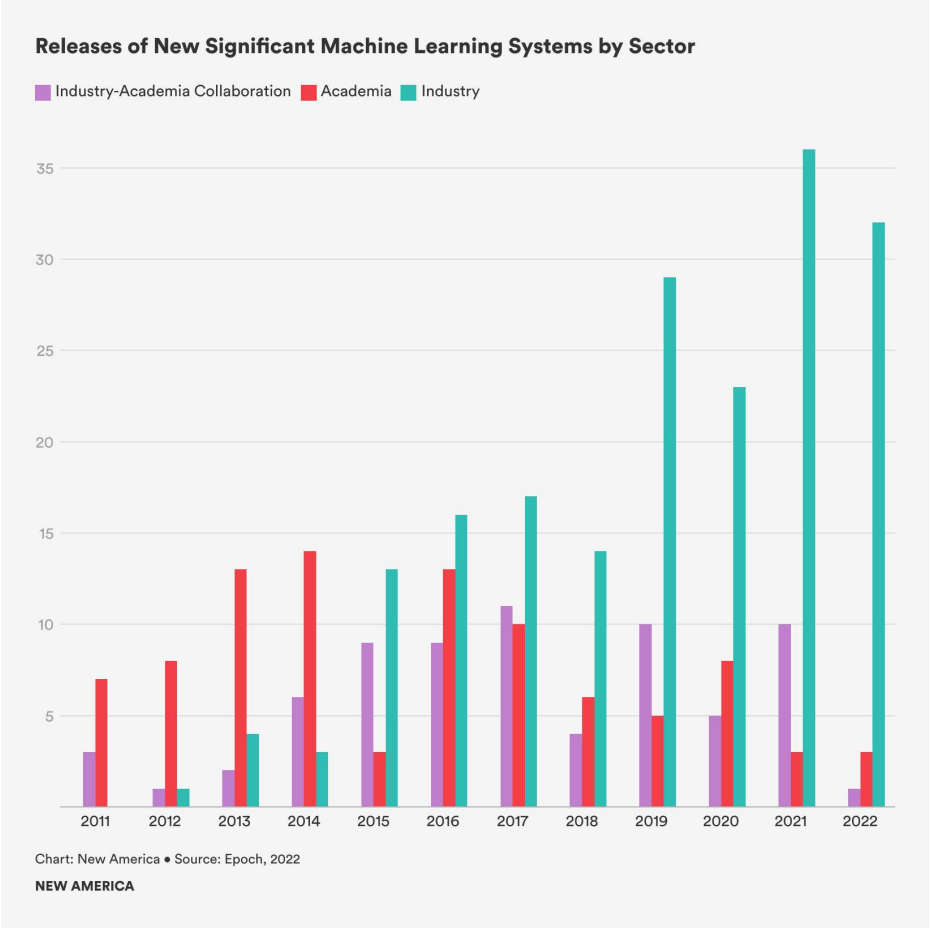
The advent of powerful generative AI systems has shaped and supercharged public and policy debates about the technology. In November 2022, the private firm OpenAI publicly released ChatGPT, a chatbot built atop a so-called large language model, which trains a layered neural network on massive datasets in order to predictively generate text or code. ChatGPT was at the time the fastest-growing consumer application in history, attracting 100 million monthly active users in two months.[12] Similarly powerful chatbots from Microsoft, Google, Meta, and others followed. Advanced machine learning systems had been on the public

radar for years, but the capability and human-like output of these generative chatbots sparked a high-profile, fractious debate about the harms and risks of AI.

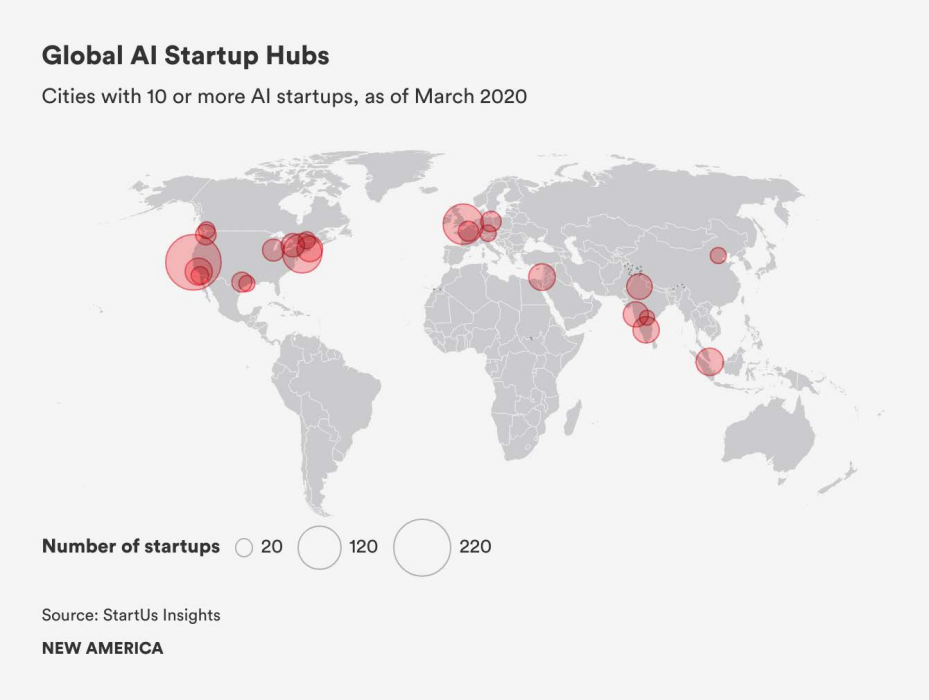
The most prominent voices in the debate are those warning of speculative, catastrophic risks of AI. Their central concern is the direct alignment problem, the question of how to ensure that an AI system pursues the goals and intentions of the humans who created it. The most extreme scenario of misaligned AI envisions a system escaping human control and pursuing goals that threaten human rights, safety, or existence.[13] A statement released by the nonprofit Center for AI Safety, that reads "Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war," has been signed by dozens of leading AI technologists, researchers, and other notable public figures.[14]

Others criticize the focus on speculative extinction risk, insisting that it distracts from—and even exacerbates—more likely and urgent risks stemming from human misuse of AI systems and their propensity to concentrate power, exacerbate structural discrimination, and further inequality.[15] AI is not a creature, but rather a set of tools, and the pressing concerns for society—researchers such as Princeton Professor Arvind Narayanan argue—stem not from the prospect of a rogue AI, but rather from the humans who design and deploy it. Humans might build and use AI tools in harmful or malicious ways, such as developing autonomous weapons systems, producing sophisticated disinformation, or distributing the knowledge to create biological, chemical, or cyber weapons.[16] Less directly, a system will express the worldview and interests of its creator in ways that can harm others. As political theorist Langon Winner noted, all technologies "have politics," in that they reflect the preferences and biases of their creators.[17]

Right now, the prevailing source of such bias in AI systems is that they are being developed primarily by white, American men in the service of private and corporate interests like profit and shareholder returns. A decade ago, universities developed most of the cutting-edge machine-learning systems, but industry now dominates.[18] The risks emerging as a result include labor market displacement, environmental damage, economic inequality, and racism.[19] These impacts disproportionately harm marginalized communities, especially in developing nations.



The global AI labor market is illustrative of these risks. Though there are emerging AI ecosystems in developing countries such as Brazil, Kenya, and India, research and development of AI systems is heavily concentrated in a handful of rich-world cities.[20] One analysis conducted at the start of 2023 found that more than 50 percent of all venture capital investments to AI startups went to companies based in the San Francisco Bay Area.[21] Yet millions of gig workers, many of whom live in the developing world, perform the menial labor necessary for building and maintaining AI systems.[22] Workers in countries such as India, Kenya, and Nigeria are paid as little as $1.50 per hour to perform tasks such as data annotation and labeling for content moderation, which often entails scrutinizing violent, traumatic videos for hours on end.[23]



Researchers and firms project the AI revolution will usher in unprecedented economic precarity, as tens or hundreds of millions of jobs might be lost to automation over the next decade.[24] And though AI systems are expected to add as much as 7 percent to global GDP by 2030, those proceeds will be unequally distributed; McKinsey Global Institute projects that rich-world AI leaders will accrue an additional 20 to 25 percent in net economic benefits, compared to 5 to 15 percent in developing countries.[25]

Thus, at the root of the AI harm debate are deep divisions along geographic, economic, social, and ethnic lines. Those who own, develop, deploy—and hence stand to be most enriched by AI systems—and dominate the risks discourse, are generally ethnic majorities from well-off cities, especially in the U.S., Europe, and China. The rest of the world—the workers, the ethnic minorities, and the poor who have little power and voice in the debate—may see their lives upended by this powerful new technology.[26] The pressing problem is not the direct alignment problem, but rather the social alignment problem—the question of ensuring that an AI system serves the goals not just of the entity that created it, but of society more broadly. Will the market be left to decide, or will governments and societies mobilize to steer the technology toward public goals?

The Digital Futures Task Force working group on AI developed a taxonomy of AI harm. This taxonomy is broad enough to pertain to different jurisdictions, countries, and groups and can be applied to present-day systems and those of the future.

1. **Input harms** refer to those stemming from a system's inputs (i.e., the datasets used to train AI models). The data—whether individual images labeled by humans or massive amounts of online text ingested by large language models—have an embedded substrate of systems of thought, culture, and power. One working group member quipped that "historical data doesn't have the luxury of historical amnesia." Other harms can emerge when training data do not represent the context where a system is being used. For instance, a farming AI trained on European agricultural data would be ill-suited for Africa. Definitional disconnects—"justice," for example, means something different in Islamic thought than it does in Western thought—raise a fundamental epistemological problem, as much of the world's potential training data reflect only two intellectual traditions: the Western, Judeo-Christian and the Eastern, Confucian. As algorithms adjudicate and implement more and more activities, other traditions of knowledge risk further marginalization.

2. **Design harms** emerge from how an algorithm is built and who builds it. Some look to the idea of participatory design to mitigate potential design harms, as many researchers, policymakers, and even industry technologists admit the need for more diverse design teams and civic participation. Our working group, however, noted that participation is a luxury enjoyed by educated, socioeconomically well-off elites. When it does occur, participation is often meaningless, as it does not automatically translate to ownership or influence.[27]

3. **Procedural and access harms** arise when opacity, inscrutability, and secrecy surrounding the use and process of an AI system in decision-making violates individuals' procedural rights. In various settings, such as hiring or criminal justice, an AI system could be used to make a decision about individuals without their awareness, leaving them unable to challenge its use. Further, the operations of many complex algorithmic models are either hidden from public view or so complex as to be inscrutable, which precludes the possibility of identifying errors and making a case for redress.

4. **Outcome harms** describe the adverse physical, social, economic, and psychological range effects of negative consequences that arise from the application and deployment of implementation of AI. These can include physical, social, emotional, and economic damages resulting from system outcomes such as autonomous vehicle accidents or the political strife caused by the spread of deepfake videos.

5. **Accountability harms** relate to issues regarding inadequate or unclear responsibility for an AI system and its actions. Who is responsible for the decisions made by an algorithm? Who is at fault when one of those

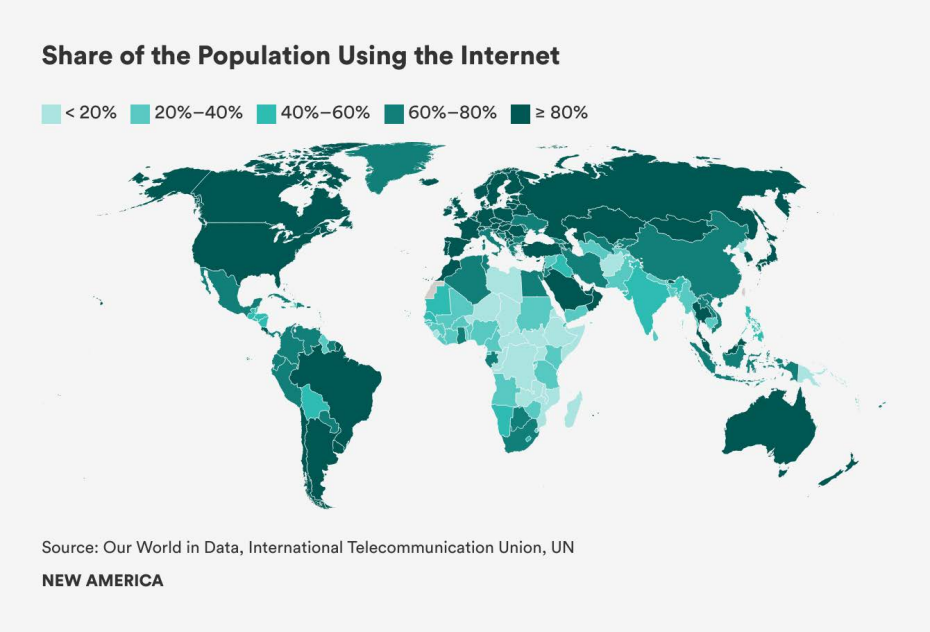
decisions causes harm? Various mechanisms may help ensure accountability, such as liability laws and algorithmic auditing.[28]

Digital Access and Divides

Digital divides encompass disparities in infrastructure and investment in digital technologies between the rural and the urban, between developing and wealthy nations, and among different socioeconomic and identity groups within societies. While wealthy countries push forward into new digital frontiers such as AI, developing economies still have limited access to digital markets, technologies, and broadband, as well as slower internet speed and a lack of opportunities for digital entrepreneurship.

The most fundamental barriers to digital access are physical: unreliable electricity, lack of wired internet access, and other network infrastructure shortcomings. For example, more than 63 percent of internet exchange points (IXPs), the physical infrastructure that maintains local internet traffic and reduces the costs and latency associated with long-distance traffic exchanges between internet service providers (ISPs), are located in Organization for Economic Cooperation and Development (OECD) countries.[29] For example, Sweden has nine IXPs, while Colombia, a country 2.5 times larger in size, has one.[30] This infrastructure imbalance translates to higher internet traffic costs and slower internet speeds for those in developing economies.

Internet access is similarly divided by geography, with most of the 2.7 billion unconnected located in the developing world.[31] Internet penetration is 89 percent in Europe, over 80 percent in the Americas, and 70 percent in the Arab states, compared to 61 percent in Asia and 40 percent in Africa.[32]



Differences in internet connectivity and use also extend to gender, age, and rural versus urban populations. As of May 2023, there were 310 million fewer women accessing the internet than men, with women 7 percent less likely to own a mobile phone and 19 percent less likely to use mobile internet than men.[33] Younger populations are more likely to be online, with 75 percent of global youth (aged 15 to 24) connected to the internet, compared to 65 percent of the rest of the population.[34] In 2021, the number of internet users in urban areas was double the number in rural areas.[35] Research has demonstrated significant positive associations between internet use and wage growth, which indicates that certain digital skills and behaviors were rewarded by the labor market.[36]

Though all of this data paints a clear picture of the digital divide, there are disagreements around the definition of *access*. In multi-stakeholder forums such as the Internet Governance Forum (IGF), representatives from wealthy nations have dominated the discussion by framing access as a human rights issue, rather than focusing on more immediate concerns such as the need for infrastructure and investment.[37] The wider debate over how to expand access is a clash of two visions, the "free market" view, often promoted by large companies, versus "universal service," whereby a government ensures all citizens have access to the internet. In addition, wealthy nations prioritize issue areas related to internet use and coordinated security policies, while developing nations are concerned with the high costs of international internet traffic and infrastructure development.[38]

"The wider debate over how to expand access is a clash of two visions, the 'free market' view, often promoted by large companies, versus 'universal service,' whereby a government ensures all citizens have access to the internet."

The task force also noted that having access does not necessarily mean freedom of use. Even with physical access to the internet, the design and control of digital infrastructure can prevent free use. The prevailing paradigm of internet infrastructure design and ownership, which is highly centralized, enables shutdowns, which occur when an ISP or government deliberately terminates access to the internet. ISPs are few, and in many jurisdictions they are state-controlled, which concentrates decision-making related to internet access, online content, and cost.

Beyond access are overlapping divides in digital skills, digital use, quality of infrastructure, and content availability. The International Telecommunication Union (ITU) organizes its goals for bridging the digital divide into two categories: *universal* connectivity and *meaningful* connectivity.[39] It identifies physical, financial, socio-demographic, cognitive, institutional, political, and cultural factors that affect access.[40] Despite the multilateral body's efforts to build consensus among nation-states, there is a lack of alignment among governments, technology companies, start-ups, and nonprofits on the root causes, definitions, issues, and consequences of the digital divide and the overall digital economy. Without harmonization, collaboration has been difficult, as each stakeholder has a limited view of what is a multifaceted issue.[41]

Geopolitical tensions pose another challenge, especially as technology becomes increasingly central to the power struggle between the U.S. and China.[42] One of the battlefields of this strategic competition is access to the internet itself, particularly in the developing world, which is highly reliant on American, Chinese, and European digital infrastructure. As part of its Belt and Road Initiative, China has invested heavily in building digital infrastructure for developing nations; its investment in the African technology sector totaled $7.19 billion from 2005 to 2020.[43] Chinese telecoms have been building submarine cables in the developing world, including a 12,000-kilometer cable connecting Pakistan, Europe, and East Africa (called PEACE) that will be maintained by Huawei.[44] Chinese hardware frequently includes surveillance technologies, which allows governments, as well as the Chinese, to collect data and manipulate online content, which poses a threat to democracy.

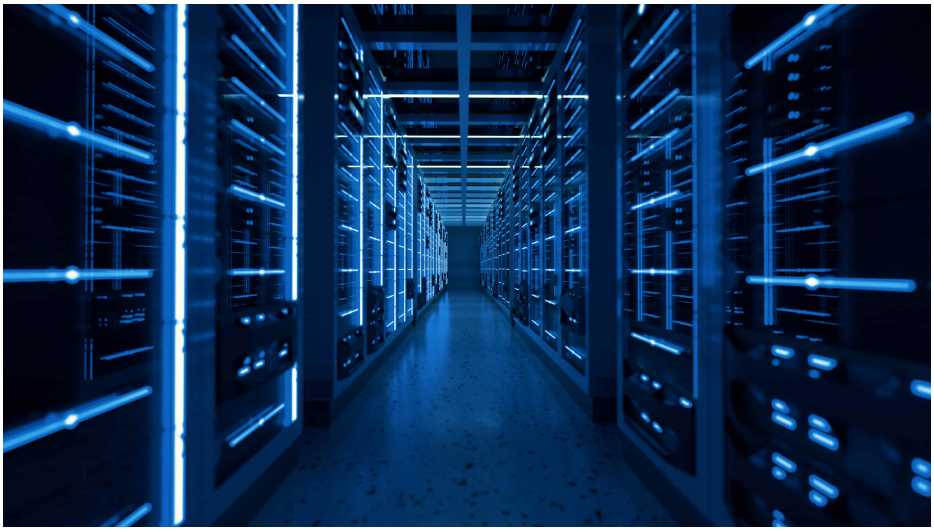
Mobile phone advertisement in Kampala, Uganda: January 23, 2018.

Source: Shutterstock

To counter China's expansion, the U.S. is rallying G-7 nations, the World Bank, ITU, and American and European companies to increase investment in submarine cables.[45] It is also using the threat of sanctions to deter countries from accepting Chinese projects.[46] Tech giants such as Alphabet, Meta, and Microsoft stand to benefit from increasing U.S. efforts to build digital infrastructure in the developing world, as more bandwidth in the developing world translates to more hours on their platforms and thus more ad revenue.[47] However, some researchers warn that if the future of the infrastructure of the internet is entrusted solely to monopolistic technology corporations, the internet will become an ever-more commercialized space primarily serving the financial interests of a handful of companies.[48]

Issues of power and justice, meanwhile, remain perennial. Wealthy nations are often the producers of digital technologies and infrastructure and designers of virtual worlds and experience, while developing nations are perpetual consumers. Developing countries are caught between either relinquishing digital sovereignty and giving up control of internet infrastructure or continuing to endure high international traffic costs and slow internet speeds. Some observers call this state of affairs "digital colonialism," the twenty-first century version of the nineteenth century "Scramble for Africa," where imperialist nations sought to divide, conquer, and exploit the whole continent for resources.[49] In an ominous echo of colonialism's tainted past, today's subsea cables often follow the same shipping routes of the colonial powers in the original contest.

Data Protection and Data Sovereignty



Source: Shutterstock

Data protection refers to a set of norms regarding the acceptable use, transfer, and ownership of data that extend beyond the concept of privacy. It has been defined in conflicting ways in various countries.[50] The European Union (EU) put forth the most widely accepted definition via the General Data Protection Regulation (GDPR), which treats data protection as a stand-alone right and addresses the abuse, collection, and processing of personal data.[51] The GDPR sets limits on data collection, storage, and processing, and creates enforceable standards for lawfulness, fairness, accountability, and transparency.[52] It also includes the "right to be forgotten," whereby users can demand that a company remove their data completely.

Although the European definition has gained traction globally as countries seeking to maintain cross-border data flows with the EU have adopted similar regulations, other nations challenge the European conception of data protection. The U.S. lacks comprehensive federal data protection legislation and has only sector-specific laws that protect education or health data, for instance. Some U.S. states, such as California have begun to debate and embrace some of the definitions and approaches encompassed in the EU GDPR model. India recently passed a bill for data protection similar to the GDPR; however, it also allows state access to data under certain circumstances, which are determined by the government, without public input. China has a strict data protection policy, but, like India, allows government access to personal data and, unlike India, restricts cross-border data flows.

As a starting point for mapping the global fault lines in this area, the task force began by disentangling the terms *data privacy* and *data protection*. Notions of privacy are grounded in values and norms and vary widely among different cultures, so it would be difficult for a shared understanding of data privacy to emerge and form the basis for a global data protection governance framework. As a general approach, the group determined that discussions about data protection must start with values, then move to rights, and finally consider implementation.

Related to data protection is the notion of *data sovereignty*, which is also a contested term that came into vogue after former National Security Agency employee Edward Snowden disclosed the U.S. and U.K. governments' metadata surveillance program.[53] A basic definition of data sovereignty is "a state's ability to control data originating and passing through its territory."[54] Because cyberspace transcends geographic borders, it poses a direct challenge to the prevailing terrestrial nation-state conception of sovereignty as geographically bound quality determined by international or regional agreement. Other literature describes data sovereignty as it relates to the individual, with some authors likening it to bodily sovereignty endowed to citizens per Enlightenment conceptions, particularly when it comes to health data, and tying it to the right to personal data protection.[55] Across the scholarly discourse, the prevailing themes when it comes to data sovereignty are control and power: Who has sovereignty over different kinds of data, and what can those entities do with that data?

Among nations, data sovereignty is a highly contentious issue. The EU believes that states should have control over the data of its citizens to protect their rights from the overreach of corporations, law enforcement and intelligence agencies, and government regulators. The U.S., on the other hand, sees the control of data as conferring national economic and security benefits and protecting the U.S. from foreign adversaries.[56] After the Snowden revelations exposed the extent of U.S. data abuse on national security grounds, this divergence broke out into the open, as the EU terminated the "EU-U.S. Safe Harbour Agreement" and subsequently the "Privacy Shield," which served as the legal frameworks for regulating cross-border commercial data flows between the EU and the U.S.[57]

In July 2023, the EU and U.S. came to a new adequacy decision under the EU-U.S. Privacy Framework, which European officials claimed is a "very robust solution" to a long-standing legal debate. However, Max Schrems, an Austrian activist whose legal challenges to the past two privacy frameworks led to their invalidation by the Court of Justice of the EU, has announced that he will challenge this latest iteration.[58] The survival of the agreement, as well as any prospective successors, will likely remain in question so long as the U.S. continues to collect the data of foreign nationals under Section 702 of the Foreign Intelligence Surveillance Act.[59] At the core of this disagreement is the desire to exercise control over data.

Nation-states attempt to control data by implementing data localization measures, whether for purposes of national security, law enforcement, or influence over the private sector.[60] For example, in China, the Data Security Law bans the transfer of all types of data within China to foreign legal or enforcement authorities, unless approval is granted by Chinese government officials.[61] While China has strict laws protecting citizens' data from foreign extradition, there are no regulations that protect citizens' data from the Chinese government. Despite China's efforts for stricter control over data generated within its territory, the government itself is not bound by the same limitations.[62]

Harm related to data protection and data sovereignty does not necessarily require the actual misuse of data, such as when data are used to generate predictions about individuals. Even perceptions of data-related harm have deepened distrust between developing nations, powerful countries, and big tech firms. That distinction led the Digital Futures Task Force working group to develop a taxonomy of harm that distinguished between perceived versus measurable harms. A measurable harm might be the use of health data to drive up insurance premiums.

Perceived harms, on the other hand, are grounded in the values of the individual or community. An absence of trust in a digital technology would count as a perceived harm. Furthermore, these harms can occur at different levels: individual, group, societal, national, and geopolitical. An individual may experience harm through a loss of privacy or the misuse of personal data to predict a certain behavioral outcome. A group harm could manifest as an algorithmic bias against a marginalized community, such as immigrants. Societal harm could arise from interference in political processes. Geopolitical harm could be an imbalance in the benefits derived from the data economy between wealthy and developing nations.

"The global, open internet relies on cross-border data flows. Impeding those flows for reasons of security or sovereignty reduces the openness and innovation potential of the internet."

The task force identified the top three areas of contestation in the global debate over data: cross-border data flows, usability, and value. The global, open internet relies on cross-border data flows. Impeding those flows for reasons of security or

sovereignty reduces the openness and innovation potential of the internet. The usability of data determines its potential benefit and so determining usability is a fault line in data protection. Finally, the appraisal of value—how data are appraised and who is doing the appraising—raises questions about the beneficiaries of data-generated value and the equitable distribution of such gains. At the moment, the economic benefits from data extraction and processing primarily accrue to private firms, which are predominantly located in the U.S. and China. The central conflict over data sovereignty arises from the inherent asymmetry of power between those who create the data and those who extract and control the data.

Digital Identity and Surveillance

Digital identity systems, which are an online representation of a person's attributes and credentials, can bestow economic and political opportunities on vulnerable populations while also enabling government or corporate surveillance. More than 850 million people, most of whom live in low-income countries or are members of marginalized populations, lack official identification.[63] As a result, they are often invisible in the eyes of the state and face economic and legal deprivations, such as the inability to open a bank account; barriers to accessing government services such as social assistance payments and health care; forced eviction; and the threat of judicial and legal abuses.

A digital ID based on biometric data, such as fingerprints or iris scans, can enable governments and nonprofits to identify and deliver benefits to populations in a way that minimizes fraud or inaccuracy. But these systems also introduce the risk of harm, such as privacy violations, personal data abuse, discrimination, and potential for human rights abuses. Debates about digital ID are most salient in the context of development and humanitarian assistance.

Proponents point to benefits, such as access to social services. The government of India's population-wide digital ID system Aadhaar has expanded financial inclusion and improved the targeting of welfare payments.[64] International organizations such as the UN High Commissioner for Refugees (UNHCR) routinely use digital ID to deliver food and cash assistance to refugees and internally displaced populations.[65] But critics note that digital ID systems can enable surveillance to exploit vulnerable populations. Governments might use digital ID programs to identify and persecute minorities.[66] Humanitarian organizations often contract the development and maintenance of digital ID systems to private corporations, which can introduce risks related to data protection and abuse.

Some scholars argue that these arrangements perpetuate a form of "technocolonialism," whereby the extraction of data from aid recipients enables multinational corporations to exploit vulnerable populations and experiment

with emerging technologies.[67] There are deep power inequities present in these transactions, as refugees, asylum seekers, and other vulnerable peoples are measured and translated into data in exchange for aid.[68]

Digital identity can lead to harms such as increased surveillance, including concerns over how data are collected and used in creating personal and group generalizations. In addition to surveillance, this practice of labeling is often done for marketing purposes. Digital identities provided by nonprofits or international organizations can also crowd out national legal identification. For instance, in providing digital identities for refugees, UNHCR alleviates pressure on host states to grant citizenship rights to stateless persons. Finally, as there are significant asymmetries in technical capacity in developing countries, governments often contract private foreign firms to develop and maintain digital identity systems. For example, Huawei employees are stationed in Kenyan police bureau offices and Kenyan biometric data is located in Shanghai as a result of this partnership.

Source: Unsplash/Gilles Lambert

Digital surveillance has become a feature of modernity. In his 2007 book *Surveillance Studies*, the Canadian sociologist David Lyon describes surveillance as "the focused, systematic, and routine attention to personal details for the purposes of influence, management, protection, or direction."[69] Scholars have different perspectives regarding the extent to which digital surveillance represents a contemporary manifestation of Jeremy Bentham's panopticon, a prison architecture in which inmates are watched from a tower in which the

watcher is not visible.[70] While some argue that digital surveillance adheres to the fundamental dichotomy of the "watcher" and the "watched," others contend that it aligns more closely with the notion of a "surveillant assemblage," in which individuals are transformed into discrete data flows and are subsequently reassembled as virtual "data doubles," targeted for behavioral intervention.[71] These conceptions, plus the use of surveillance in totalitarian regimes, carry negative connotations, but digital surveillance can yield societal benefits. For instance, surveillance is used to manage and contain disease outbreaks as well as prevent crime.

But states and corporations also use digital surveillance to repress populations, violate rights to expression and privacy, and extract value from individuals. Autocratic states, especially, use digital surveillance systems in a manner that evokes the panopticon.[72] Perhaps the most extreme example at the moment is in the western Chinese province of Xinjiang, where the state uses a pervasive surveillance system involving biometric and digital checkpoints, tracking apps, big data processing systems, and social behavior data gathering to control the Muslim Uyghur minority.[73] This type of surveillance aims to internalize control, morals, and values within the population, reinforcing the state's disciplinary power.

Western democracies also surveil their citizenry for "national security" purposes. Although Snowden's disclosures of widespread surveillance of U.S. citizens eventually led to Congress banning the practice, the U.S. government still routinely surveils the public. According to a 2021 report by the Office of the Director of National Intelligence (ODNI), 3.4 million warrantless searches of Americans' phone, email, and text records were conducted in 2021, as a result of Section 702 of the Foreign Intelligence Surveillance Act.[74]

In June 2023, ODNI reported that the U.S. government was voiding the Fourth Amendment by purchasing private data through data brokers. This report asserted that the "U.S. government believes it can 'persistently' track the phones of 'millions of Americans' without a warrant, so long as it pays for the information."[75] States also partake in this practice, particularly in monitoring social media accounts. Harms associated with these activities include eroding privacy, stifling open communication online due to fear of being monitored, misinterpreting the significance of social media activity, or erroneously attributing criminal conduct based on social media engagement.[76] Because of long-standing societal biases, communities of color face an increased risk of surveillance, which exacerbates discrimination and perpetuates power inequities.

In the digital surveillance industry, the separation between the public and private sectors has become blurred. Private firms often carry out government-led surveillance, and corporate surveillance only exists in a conducive regulatory environment. Private companies have pioneered a lucrative business practice known as "surveillance capitalism."[77] Shoshana Zuboff, an American social

psychologist and well-known critic of the tech industry, describes surveillance capitalism as a "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales."[78]

Corporations gain access to personal data through their terms and conditions service agreements in which users give away their privacy in exchange for a free online service, such as access to friends' photos or medical and legal advice. Sometimes, companies do not even ask for permission; Google's Street View deploys cameras to take photos of people's private residences without gaining consent from property owners.[79] This asymmetry of knowledge between surveillance capitalists and users results in an asymmetry of power, as there is little to no oversight of these practices. Zuboff calls this imbalance "instrumentarian power," which is a "ubiquitous, sensate, computational, actuating global architecture that renders, monitors, computes, and modifies human behavior."[80]

Transnational Cybercrime

Ever since computer systems have been networked, there has been criminal activity occurring on them. In 1983, when the internet's predecessor, the Advanced Research Projects Agency Network (ARPANET), was still relatively small, the Federal Bureau of Investigation arrested a group of six young men who had used personal computers and dial-up modems to hack into, and in some cases damage, more than 60 computer systems, including at the Los Alamos National Laboratory.[81] A year later, an informant estimated that each year hackers were committing $200 million in credit card fraud and stealing $100 million in software.[82]

As the globalized internet has expanded, so has transnational cybercrime, proliferating to encompass a wide range of harmful activities targeting computer systems, critical infrastructure, organizations, and individuals. This type of crime has become more sophisticated, commercialized, and pervasive. Whereas most cybercrime was once carried out by individuals or groups of hackers, researchers and law enforcement officials have documented a rise in online criminal groups that regulate or control the production or distribution of a specific illicit product or service, much in the same way a mafia supplies protection or a cartel distributes narcotics.[83]

Accurate data are hard to come by for the scale and scope of cybercrime, but credible estimates say that damages increase 15 percent per year, going from $3 trillion in 2015 to a projected $10.5 trillion by 2025.[84] Of particular note, ransomware attacks, whereby an attacker uses software that encrypts a user's files and demands payment in exchange for the key, were up 62 percent worldwide from 2019 to 2020, with costs from these attacks increasing more than 60-fold, from $325 million in 2015 to $20 billion in 2021.[85] In 2021, U.S. security

agencies reported observing ransomware incidents in 14 of 16 critical infrastructure sectors.[86] The highest profile of these was an attack that forced the temporary shutdown of 5,500 miles of the Colonial Pipeline on the East Coast, causing gasoline and jet fuel shortages that triggered a rise in gas prices.[87]

Though cybercrime is an ever-worsening global challenge, there is no precise definition of or consensus on what constitutes a cybercrime, nor are there agreed-upon classification systems that can account for the range of profit-seeking, ideological, and malicious cyber-activities that could qualify.[88] In scholarly literature, the two most-cited definitions of cybercrime are (1) "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" [89] and (2) "any crime that is facilitated or committed using a computer, network, or hardware device."[90] Such definitions are so vague as to lack utility, which has led researchers and policymakers to rely on various, often competing, classification systems. The most basic of these distinguishes between "cyber-enabled" crimes—traditional crimes such as money-laundering, drug trafficking, or terrorism that are facilitated by digital technology—and "cyber-dependent" offenses—crimes such as distributed denial-of-service or ransomware attacks that only exist in the digital world.[91] Others establish even more categories.

This definitional ambiguity has implications in the worlds of policy and law. Regulatory and legal regimes vary widely across jurisdictions, confounding attempts at international cooperation and legal harmonization.[92] The transnational nature of the digital domain means that cyber criminals can move their operations to less-regulated jurisdictions.

Government attempts to harmonize national laws have faced opposition. The Council of Europe, with participation from Canada, Japan, the Philippines, South Africa, and the U.S., drew up a legally binding treaty known as the Budapest Convention that opened for signature in 2001. The Convention established 14 different cybercrime offenses grouped under a four-category classification system, to which a fifth category was added in 2003: (1) Offenses against the Confidentiality, Integrity, and Availability of Computer Data and Systems; (2) Computer-Related Offenses; (3) Content-Related Offenses; (4) Offenses Related to Infringements of Copyright and Related Rights; and (5) Acts of a Racist and Xenophobic Nature Committed through Computer Systems.[93]

Members of the Digital Futures Task Force working group on cybercrime agreed that this taxonomy was out of date and too technical. It omits a range of harmful cyber-related or cyber-enabled criminal activities, such as election interference and other political crimes and various forms of online hate speech. As of 2021, only 68 nations were party to the Budapest Convention. Some non-signatory nations agreed with the content of the Convention but not the process by which it was created. India, for instance, cooperated with the Council of Europe to bring its cybercrime legislation in line with the Budapest Convention in 2008, though it

refused to sign, in part because it did not participate in its negotiation.[94] Autocratic states, many of which sponsor transnational cybercrime activities, opposed the principles of the Convention and organized to undermine it. Russia is the leader of this effort. Although Russia was a member of the Council of Europe at the time the Budapest Convention was negotiated, internal domestic views on the part of the ruling regime in the Kremlin have colored Russia's subsequent criticism of the Budapest Convention. Before Russia exited the Council of Europe in March 2022 on the heels of the war in Ukraine, Kremlin representatives claimed the treaty violated state sovereignty by enabling cross-border cybercrime operations.[95]

In 2019, Russia, along with Belarus, Cambodia, China, Iran, Myanmar, Nicaragua, Syria, and Venezuela, presented a resolution to the UN General Assembly calling for the establishment of an international convention to combat cybercrime.[96] Though the U.S., EU, and other signatories to the Budapest Convention opposed the motion, the resolution passed, leading to negotiations that, as of this writing, are ongoing. Language in the resolution, as well as a Russian draft treaty backed by China, proposed a vague definition of cybercrime, prompting the assertion by the U.S., EU, and other states, as well as human and digital rights groups, that the intention of this resolution was to give cover for autocratic states wanting to criminalize ordinary online expression and to exercise greater state control over the internet.[97] The Russian-led effort to establish an international cybercrime convention at the UN is part of a larger campaign that autocracies are waging in international fora such as the International Telecommunication Union, to change global cyber norms and governance, such that the internet is brought under greater state control.[98]

In the view of the Digital Futures Task Force working group on cybercrime, a useful global-consensus taxonomy of cybercrime would be nearly impossible. Putting aside the fact that some states sponsor transnational cybercrime, different regions and groups experience cybercrime differently. Norms surrounding privacy and acceptable speech vary from one jurisdiction and culture to another, for instance. In addition, technical literacy and capacity determine the real and perceived harm of a cybercrime. Low-income countries might have justifiably little interest in passing cybercrime legislation when lack of broadband access or electricity are more pressing concerns for the population.

A more tractable approach, therefore, might be to define and categorize cybercrime on a regional basis. Venues for such efforts already exist. For instance, since 2013, the Association of Southeast Asian Nations (ASEAN) has convened a Senior Officials Meeting on Transnational Cybercrime to coordinate regional approaches to cybercrime, share information, conduct training, and carry out capacity-building activities. But the group agreed that the borderless nature of digital space confounds a regional approach. Criminal activity would shift to the most lenient, and, in many cases, the most vulnerable parts of the world.

One solution to this problem could be to distinguish between technical cybercrimes and social cybercrimes. Technical crimes—offenses against the confidentiality, integrity, and availability of computer data and systems—are universally measurable and consistent, whereas social cybercrimes are context-dependent. This leads to the idea that instead of focusing on the supply side (i.e., the perpetrators of cybercrimes), one could base a definitional framework around the demand side—the targets and victims. A definition rooted in this approach might stand a better chance of global acceptance, while allowing for local variation and national self-determination. The autocracies that sponsor and enable transnational cybercrime would still defect, but a demand-side framework might also encourage a greater emphasis on demand-side governance solutions: capacity building, victim compensation, and cyber awareness and education. As a practical matter that might be a more promising governance approach, since, so long as autocracies continue to enable transnational cybercrime, curbing the global supply of cybercriminal activity will be a challenge.

The Global Digital Governance Map

Currently, a patchwork of national regulatory regimes, multilateral bodies, corporate policies, and multi-stakeholder organizations governs the various layers of the digital domain. Internet governance has traditionally fallen to the private sector and technical community, as internet service providers and telecommunications companies built and own much of the world's network infrastructure. Among nations, there is little agreement over the rules of cyberspace. The establishment of the World Wide Web in 1991 came at the start of a short-lived period of American hegemony, and as the internet expanded globally nations mostly deferred to U.S. norms for cyberspace. But as the world has become multipolar in the twenty-first century, governance of the digital domain is an increasingly contested front line in geopolitical power struggles.

Different nation-states now have distinct and divergent digital governance models. The three major standard-setters are the U.S., European Union, and China. The U.S. prioritizes the interests of the firm, regulating lightly and allowing tech companies wide remit to govern, innovate, and acquire power. The EU puts more stock in the interests of consumers, or end users, by using its regulatory might to impose protections and limit anti-competitive corporate practices. In China, the state takes precedence, as the digital economy is made to conform to the ideological and policy goals of the autocratic Chinese Communist Party. Other nations have for the most part followed one of these models, or adopted elements of each, though a distinct fourth approach is emerging in India, which, through public-private partnerships, has developed the world's most extensive national digital infrastructure to drive economic development and inclusion, at times at the expense of individual rights and liberties.

Multilateral bodies, especially those housed in the UN system, such as the International Telecommunication Union (ITU), play a critical role in setting worldwide technical standards and managing network infrastructure. Increasingly, these fora have become arenas for competition between Western democracies and their allies and authoritarian states, such as Russia and China, which seek to exert greater control over the global internet. Amid this power struggle, good-faith multilateral efforts to develop international treaties and definitions have stalled or failed.

In the absence of global rules, multinational technology companies have created their own governing regimes. Tech behemoths such as Meta and Google, with trillion-dollar-plus market capitalizations and billions of people worldwide using their products, enact policies that would typically be the purview of governments, such as regulating international payments and commerce and determining the limits of free speech.

Because the internet is a public, private, and civic enterprise, many point to multi-stakeholderism as the archetype for governing the digital domain. Already, bodies that bring together governments, civil society, the private sector, and the technical community perform essential governance functions. The preeminent example is the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit that manages the address book of the indexed internet and without which the web would cease to work.

The United States: Laissez-Faire, Market-First Techno-Capitalism

The de facto standard-setter for global digital governance is the U.S., which takes a laissez-faire approach that is conducive for innovation and growth but offers scant protection to consumers and allows extensive harm to users and institutions. The internet was developed in the U.S. with government backing in the 1960s. It evolved principally from the Department of Defense Advanced Research Projects Agency Network (ARPANET) project. Its principle inventors sought to be able to quickly and smoothly enable the exchange and transfer of information across remote decentralized networks of computer terminals. Its formation involved universities, companies, and scores of independent researchers and technical experts.

The functional design of the internet's architecture was open and interoperable, with open protocols allowing different devices and networks to plug in and for anyone to build tools and services. A hands-off approach enabled this ecosystem to flourish, and though the U.S. government has played a governance role—the U.S. Department of Commerce supervised ICANN until 2016, for instance—it generally has allowed the digital domain to remain an open system of information exchange. A techno-utopian libertarianism (what two social theorists in 1996 called the "Californian Ideology") prevailed in Silicon Valley, furthering the notion that government interference in the digital economy would threaten innovation and growth.[99] This mindset persists: In unveiling a framework for AI legislation in June 2023, Senate Majority Leader Chuck Schumer emphasized, above all else, that AI regulation must "prioritize innovation."[100]

Aerial photo of Apple campus building in Cupertino, CA: December 13, 2017.
Source: Shutterstock

U.S. tech regulation reflects this idea that "less is more." Legal doctrines that have curbed the power of other industries have not applied to internet companies. The consumer welfare standard that informs antitrust law, which defines monopolistic behavior in terms of financial harm to consumers, does not apply to free services such as online search or social media. Section 230 of the Communications Decency Act of 1996 shields tech firms from liability for content posted on their sites and platforms. Though Section 230 facilitated the growth of an open internet by allowing user-generated content to flourish—services such as Wikipedia could not exist without it—it also has enabled tech platforms to elude responsibility for harmful content posted on their sites, not just at home but abroad. Even if these companies are sued by users in other nations, they are free from liability in their home country.

Most digital regulation and policy is state- or sector-specific. For example, the federal government has enacted data protection and privacy legislation in sectors such as health and education—through the Health Information Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), respectively. Regulations like HIPAA have limited applicability beyond medical and insurance providers. If someone searches for a medical condition on Google, HIPAA does not protect that person's private health data from being collected, stored, and exploited. In the absence of comprehensive federal data protection legislation, a number of states, such as California, Colorado,

Connecticut, and Virginia, have enacted their own regulations, with many additional states poised to implement legislation in the coming years.[101]

The one area where the federal government has taken a more active approach to tech regulation is in national defense vis-à-vis China. In response to what is perceived to be a national security threat, the government banned the sale of equipment produced by Chinese company Huawei in 2022. The U.S. claims that Huawei has violated international sanctions and its equipment could be used to conduct cyber espionage.[102] The U.S. federal and state governments have also banned Chinese social media platform TikTok on government-owned devices. Montana has banned the app outright, and it will no longer be available for download in the state starting in 2024.[103] These policies are symptomatic of a fear, perhaps misplaced or exaggerated, that the Chinese government will be able to access commercially-acquired information of American citizens, posing a threat to national security.

American influence on global digital governance stems in part from the expansion of U.S.-headquartered tech firms abroad. The capital power held by American tech companies allows the U.S. to co-govern the digital world. While this growth has historically yielded advantages, such as the promotion of American values like free speech, the concentration of power among American big tech companies marginalizes those who were not initially considered during the system's design, raising concerns about diversity, equity, and inclusivity online. The exportation of the Silicon Valley model has led to a proliferation of harms, leaving users vulnerable and lacking recourse against large multinational tech corporations that operate with limited oversight in areas such as content moderation and data collection. Several nations have undertaken measures to rein in "Big Tech" and assume responsibility in areas where the U.S. government has been absent.

The European Union: User Sovereignty above All

The EU has taken a heavy-handed approach to digital regulation in the interest of protecting the rights of its users. An additional unstated, but widely acknowledged subtext of current EU regulation is the desire to mitigate potential harms posed by monopolistic behavior to the economic interests of European member states that have struggled to innovate in the digital sphere at the same rate of speed as the United States and China. From data privacy protections to AI, the EU has been at the forefront of rights-based digital governance, making it what many would consider the "world's greatest regulatory superpower."[104] Observers talk of the "Brussels Effect," which refers to non-European governments aligning their digital regulatory frameworks with those of the European market.[105]

The Brussels Effect enables the EU to be a normative power that exerts ideological influence around the world, promoting values such as democracy, respect for human rights, anti-monopolistic free markets, and responsible innovation. For example, the EU's Digital Services Act (DSA) aims to shape the values of very large online platforms (VLOPs), sites with over 45 million monthly active users in the EU. The DSA bans advertising based on profiling and using categories of special sensitive data (such as sexual orientation or religion); increases transparency in algorithmic content moderation; dictates response mechanisms when illegal content is detected online; informs users about content recommendation decisions; and requires VLOPs to perform due diligence such as risk assessments.[106] The goal of the legislation is to influence non-EU tech platforms to adhere to European value systems, at least when operating within the borders of the bloc.

Additionally, the EU and its member nations have been appointing tech diplomats to the seat of digital power in Silicon Valley, led by the appointment of the Danish Tech Ambassador in 2017. Instead of engaging with tech company public policy teams in their home country, these representatives seek to influence the firms' executives and decision-makers. Tech diplomats engage regularly with VLOPs and other companies to discuss topics like digital human rights, responsible innovation, and disinformation. In 2022, the EU appointed a digital envoy to San Francisco to act as a "digital enforcer" to help tech companies comply with legislation such as the DSA.

The EU's most recent contribution to the digital governance landscape is its draft AI Act.[107] The EU is taking an ex ante, risk-based approach to AI, attempting to regulate the technology *before* a crisis erupts. Jaron Lanier, an American computer scientist and writer, summarizes the Act as "the right to not be manipulated by computation."[108] Under the proposed legislation, the EU has developed a differentiation of harms dependent on AI risk. For example, AI systems with "unacceptable risks" such as AI for social scoring or predictive policing would be banned outright, while high-risk applications such as consumer products and AI used for socioeconomic decisions would be subject to certain requirements.[109] This bill also assigns recommender systems on social media platforms to the "high risk" category, effectively subjecting these sites to more scrutiny and increased liability for their content.[110]

The regulatory power afforded by the size of the EU common market has been a boon for the single-currency bloc, as it lacks the technological supremacy and regulatory frameworks for private industry innovation required to otherwise be a significant player in the digital realm. Research by McKinsey & Company corroborates this point: A 2022 report found that European companies underperform relative to those located in other regions as they are growing more slowly, investing less in research and development, and banking lower returns.[111] Central to the European approach is an increased desire for digital sovereignty as

the bloc seeks to bolster its private sector, which is more inclined to uphold European values compared to foreign multinational corporations.

China: Digital Authoritarianism

Public surveillance cameras on a pole in Shanghai, China: February, 19 2021.

Source: Shutterstock

The Chinese model of digital governance relies on authoritarian control to advance the ideological and policy goals of the state. This model envisions a world not of a single, open global internet, but of an internet fractured along territorial lines. "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty," declared a 2010 white paper from the Chinese State Council Information Office.[112] In practice, the Chinese Communist Party exerts significant technical and social control over cyberspace, mediating the country's connection to the global internet and maintaining the world's most comprehensive online censorship regime. At the same time, the Party has set ambitious goals for high-tech innovation, protected and policed technology companies, and driven public and private investment into the tech sector—efforts that a group of New America cybersecurity researchers say "arguably constitute the most comprehensive framework for [information and communications technology] governance currently underway globally."[113]

The government's digital control starts at the infrastructure level, where the Ministry of Industry and Information Technology strictly oversees the country's

gateways to the global internet and restricts cross-border information requests and access to servers abroad.[114] This enables what Western media calls the "Great Firewall," a massive online content censorship and surveillance apparatus that relies on deep packet inspection and other tools to block many foreign websites and online platforms and requires domestic companies, websites, and platforms to moderate and remove content deemed harmful or undesirable by the government. Though the Great Firewall has existed since 2000, in recent years it has become more expansive and sophisticated, deploying AI tools for content censorship, cracking down on virtual private networks (VPNs), giving social scores to companies, and blocking a greater array of content.[115] The government will also order ISPs and telecommunications companies to shut down internet and mobile service to quell online dissent and expression in areas ranging from entire regions to individual families.[116] Chinese authorities make extensive use of digital surveillance technologies, ranging from AI-powered cameras to biometric sensors, to both enhance the quality of life for citizens, such as by mitigating traffic congestion, and to advance social governance goals, such as to control the lives of minority populations.[117]

An assertive regulatory ecosystem aligns digital technology with state priorities. Closing off the Chinese internet to foreign tech platforms such as Google and Facebook enabled the rise of homegrown companies, such as Alibaba in e-commerce, Baidu in search, and Tencent for social media and other internet holdings. Over the past five years, Chinese regulators have taken steps to constrain the tech sector, including launching antitrust probes and levying fines; enforcing data security protocols intended to ensure that Chinese personal data collected by private companies stays in China; and curbing what leaders called the "disorderly expansion of capital" at the expense of the public interest, including halting approvals for new companies and suspending the initial public offering of financial technology company Ant Group.[118] Observers have noted that this so-called crackdown not only asserts the Party's control over big tech, but it also serves policy goals, such as macroeconomic stability and the reduction of foreign influence over the sector.[119]

As its geopolitical clout has grown, China has become a cyber norm entrepreneur, rallying not just other autocracies but also smaller countries that may feel colonized by American tech giants behind its vision of digital sovereignty.[120] Through its "Digital Silk Road" initiative, China has sold digital hardware and constructed network infrastructure in the developing world, often at a lower cost than Western competitors. At the same time, other countries, from Zimbabwe to Venezuela, have purchased Chinese surveillance technologies and sought to construct their own versions of the Great Firewall.[121]

India: Techno-Nationalism

A fourth digital governance trendsetter is emerging: India. Though still a lower-middle-income country with a per capita GDP of $2,388 and the world's largest population (at 1.4 billion), India is undergoing a rapid digital transformation. From 2014 to 2019, the digital economy grew at a rate of 15.6 percent, two-and-a-half times that of the economy overall.[122] India has made homegrown digitization a cornerstone of its national development and international identity. The hallmark of its model is a national digital infrastructure, built through public-private partnerships, that is neither laissez-faire nor entirely state-controlled.

The "India Stack," as the country's digital infrastructure is called, is a unified, interoperable software platform with government-backed application programming interfaces (APIs) upon which third parties can build applications.[123] The base layer is a digital ID system called Aadhar, Hindi for "foundation," which uses biometric and demographic data to assign each person a 12-digit identity number recognized by government agencies, banks, telecommunications companies, and others. It was developed by a team led by software entrepreneurs working within a government authority under the Ministry of Electronics and Information Technology. Launched in 2009 when only 13 percent of Indians had a verifiable identity, by June 2023 almost the entire population of 1.4 billion had a digital ID.[124]

Identity verification enables the next layers of the stack, the first of which is the Unified Payments Interface, an interoperable transactions system that links banks, mobile fintech apps, and any other online payment service to enable instant transfers at near-zero cost. Overseen by the central bank and managed by a government-backed nonprofit, the interface is used by the government to deliver welfare benefits and by people to pay bills, transfer remittances, and purchase goods. India is now the world leader in real-time digital payment transactions, recording 65 transactions per capita per year, compared with 12 in China and 8 in the U.S.[125] The next layer is a digital database called DigiLocker, in which individuals can store and share paperless documents such as driving licenses, medical records, and academic credentials. Additional layers are in development, such as the Open Network for Digital Commerce, an interoperable e-commerce system that would enable customers to order, pay for, and have delivered goods from services that are all registered to different apps, in contrast to walled-off platforms such as Amazon that control every step from seller to customer.[126]

The India Stack has driven financial inclusion, improved government capacity to deliver benefits and services, and stimulated entrepreneurship, as open, interoperable systems in payments or ecommerce, for instance, help create a level playing field that diminishes the ability for large companies to dictate terms and acquire monopolistic positions. At the same time, concerns about privacy, data security, and surveillance have arisen, as the government and companies are

gathering vast quantities of personal information with few guardrails in place. A recently passed Digital Personal Data Protection Bill will require data fiduciaries to apply adequate security measures to protect user data, but it also grants the government the authority to exempt state agencies from those provisions, a carve-out that digital rights activists argue could lead to increased government surveillance.[127]

As the holder of the G20 presidency in 2023, India has launched a diplomatic effort to promote the India Stack model and encourage its adoption across the developing world. But though the government champions its open, interoperable digital infrastructure, it also exercises control over aspects of the digital domain to promote government priorities. The government uses digital platforms to spread sometimes inflammatory Hindu-nationalist messaging and often demands those same platforms remove content of opposition parties and groups. India has banned foreign apps—Chinese ones especially—in the name of national security and digital sovereignty. According to Access Now, there were more internet shutdowns in India over the last five years than in any other nation, carried out to silence critics, prevent insurgents from organizing, and to prevent cheating in school exams or government job entrance tests.[128]

Multilateral Institutions: Sovereignty Divides and Weaponized Interdependence

In digital governance, multilateral organizations have played critical roles in setting technical standards, managing network infrastructure, and shaping cyber norms that enable an open global internet to exist. But increasingly, they are battlegrounds in which states with competing visions for the digital future vie for influence. The primary fault line is between the Western democracies and their allies who seek to preserve an open global internet, and the autocracies who wish to see states exercise greater control over the internet and extend national territorial-based sovereignty into the digital domain.

The most powerful multilateral body is the International Telecommunication Union (ITU), which was established in 1865 to regulate the telegraph industry and is now a UN specialized agency with the mandate to ensure "networks and technologies seamlessly interconnect," as well as to improve worldwide access to information and communication technology.[129] Among other things, its 193 member-states and 900 private sector members develop policy and regulations that determine the international standards for internet connectivity, 5G technology, and other information and communications networks.

ITU Council Meeting in Geneva, Switzerland: July 11, 2023.
Source: ©ITU/D.Woldu

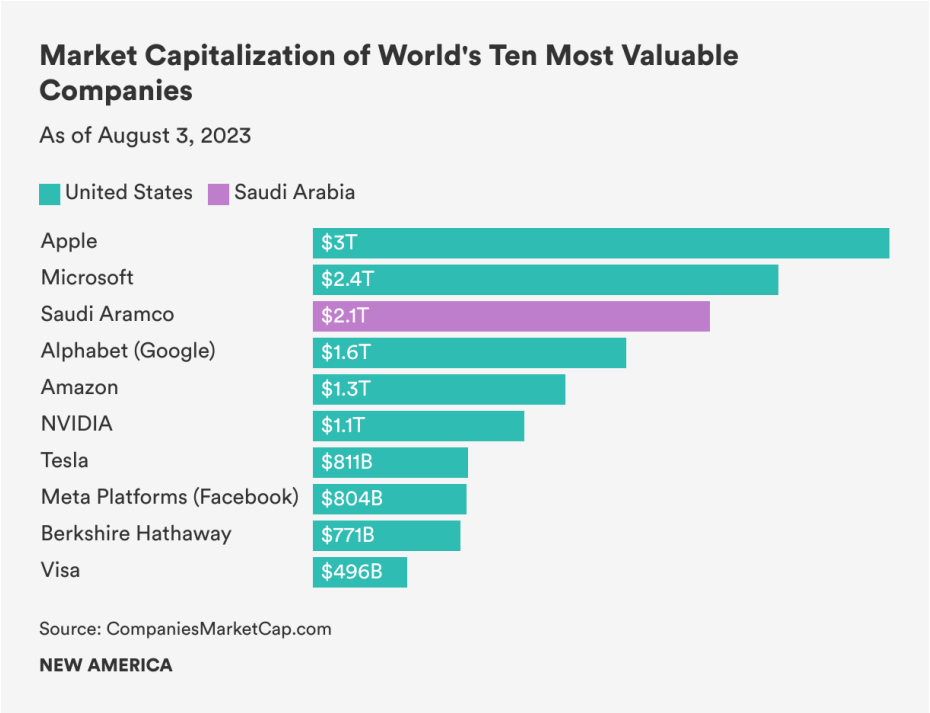
Contests over those standards have intensified, as China, Russia, and other authoritarian states have pushed an agenda at the ITU that experts say would reshape the global internet from an open, largely free network of networks to a fragmented "splinternet" controlled by nation-states.[130] China has repeatedly proposed a new internet protocol (IP) that would, among other things, require internet users to register themselves to access many online services and enable governments to more easily and quickly shut off parts of the internet.[131] According to a group of Oxford University researchers, implementation of the new IP would "splinter the global internet's shared and ubiquitous architecture"; lead to state-dominated internet governance that excludes companies and civil society; and weaken cybersecurity, enable human rights violations, and widen the digital divide.[132] The defeat of the new IP proposals, plus the victory of a U.S. representative as secretary general of the ITU over a Russian candidate, after a pitched election that pitted the authoritarian vision against the open one, has meant the preservation of the status quo, for now.

The battle within the ITU is emblematic of the war over digital governance playing out across intergovernmental organizations. Media have reported that China is pursuing a "well-resourced and widespread targeting of key, but low-ranking, positions in global digital standards agencies to push its own agenda."[133] American researchers Jeffrey Ding, Paul Triolo, and Samm Sacks describe how China's government "views standards as playing a significant role in the country's aspirations for AI leadership" and has accordingly sought to play a leadership role on the International Organization for Standardization (ISO) and

International Electrotechnical Commission (IEC) subcommittees responsible for developing these standards.[134] The fight is also playing out over the norms of cyberspace. In the UN Open-Ended Working Group, a body tasked with negotiating an international convention on cybercrime, autocracies are pushing for a broad and vague definition of cybercrime that digital rights experts say would justify greater government control over online activity and expression.[135]

Big Tech: Self-Governance and De Facto Dominance

A handful of American tech companies are the most highly capitalized, and arguably powerful, corporations in the world. Four of the planet's five largest companies are U.S. tech firms: Apple, Microsoft, Alphabet, Amazon, and Meta, with a combined market cap of more than $9 trillion[136] as of August 2023, larger than the GDP of any single nation save the U.S. and China.[137]



Big Tech's products are used by populations greater in size than that of any country. Facebook has 3.03 billion monthly active users as of June 2023; WhatsApp has 2.7 billion as of July 2023; and Instagram has 2.6 billion.[138] Some 3.6 billion use Alphabet's smartphone operating system Android.[139] YouTube, which is owned by Alphabet, has 2.7 billion monthly active users.[140] Alphabet's Google is the most visited website in the world, with 92 percent of the online search market and an estimated 4.3 billion users.[141] The ubiquity of its products

means that American Big Tech not only wields market power but it "directly affect[s] the livelihoods, relationships, security, and even thought patterns of billions of people across the globe," according to American political scientist Ian Bremmer.[142]

These companies now exert geopolitical influence that rivals states and exercise governance over domains that were traditionally the sole purview of governments. The power of Silicon Valley tech giants derives first from highly concentrated corporate control over knowledge and discourse, which in turn shapes both applications and the regulatory environment. Such so-called Big Tech power also stems from the ability of big companies with large capitalization to shape the platforms and infrastructures that facilitate and enable communication and information exchange, including through the purchase or elimination of smaller competitors and the assertion of monopolistic power over technologies that overlap with and rely on the products of multiple industries.

For instance, in 2021, Meta, in what was later revealed to be a negotiation tactic to thwart a proposed Australian law that would require the company to pay news industry outlets for their content that appeared on Facebook, briefly blocked all news on Australian Facebook as well as Australian government and hospital pages.[143] The move effectively restricted digital access to public services and information amid the country's COVID-19 vaccine rollout and wildfire season. Facebook and Twitter (now X) regularly make decisions about the acceptable limits of free speech without democratic process. The growing governance power of big tech has prompted commentators to declare the dawn of a "digital world order" and the fact that "net states [rule] the world."[144]

"While the U.S. has traditionally been the foremost exporter of democracy, it now exports the technology that has and will continue to disrupt democracies worldwide."

The highly permissive U.S. regulatory approach has enabled Big Tech to largely govern itself. The companies write their own community guidelines for content moderation, which Georgetown Law Professor Anupam Chander says are "modified only as necessary in the face of enforcement efforts by foreign governments or negative publicity."[145] Though at times aligned with and influenced by U.S. national interests and values, these corporations are, above all else, driven to maximize profit or shareholder returns, so their actions have at times led to human rights violations and the undermining of democratic norms.

Facebook's algorithms have amplified disinformation that has subverted democratic elections and led to real-world violence, such as in Myanmar where the spread of hateful content contributed to a brutal ethnic cleansing campaign against Rohingya Muslims that displaced more than 700,000 people and left as many as 7,000 dead.[146] While the U.S. has traditionally been the foremost exporter of democracy, it now exports the technology that has and will continue to disrupt democracies worldwide.

Multi-Stakeholder Bodies: Democratic Governance and Decentralized Issue Resolution

Much of the global digital commons is governed by multi-stakeholder bodies and processes that include all the players who have a role (or stake) in the functioning, performance, and outcomes of a particular technology. That may include governments, companies, intergovernmental organizations (such as UN agencies), civil society organizations, and technical experts. Multi-stakeholder bodies are inclusive, able to accommodate multiple perspectives in deliberation and decision-making processes.[147]

Governance of the internet depends on a decentralized global network of multi-stakeholder bodies. The most prominent body is ICANN, the organization responsible for managing the Domain Name System (DNS), the phonebook of the indexed internet. In the early days of networking before the global internet, connecting two computers required memorizing their IP address digits. That changed when American computer scientist Jon Postel developed the DNS, which organized the names according to their hierarchical domain (such as .com or .gov) while also storing the information necessary to translate the name into an IP address in various servers located across the globe. The National Science Foundation, a U.S. government agency, had oversight of the system until the growth of the internet in the 1990s prompted the Clinton administration to call for the privatization of DNS management to promote competition and facilitate the internet's international expansion.

In 1998, ICANN was created as a nonprofit public benefit corporation, with a globally representative governance structure developed in consultation with the government, business, technical, and engineering communities involved in managing the internet. Though it would be privately run, the U.S. government mandated that ICANN operate in a consensus-driven and democratic manner, "reflect the diversity of [the internet's] users and their needs," and "reflect the bottom-up governance that has characterized development of the internet to date."[148]

In practice, the organization is composed of volunteers from 130 countries and territories that form four advisory committees and three supporting organizations.[149] Any member of these groups can raise issues within their

organization, which are then assessed for the potential to become consensus policy after public comment. Working groups and task forces then develop policy recommendations, which are subjected to public feedback before final adoption and implementation by ICANN.[150] Voting within the organization is sometimes performed by humming, in which the side with the loudest hum is taken as the consensus of the membership.

ICANN has been essential for a stable, global internet. And its model carries lessons for multi-stakeholder governance of any digital technology. ICANN had the backing of the U.S. government from the start, which conferred legitimacy and power to the organization. It is not only inclusive, but it also affords its members ownership of processes and decision-making, since all members can introduce and vote on policy. ICANN is focused on performing specific, practical functions. It is not a talk shop, and its mandate is clearly defined. The volunteers who comprise its membership share a common technical language and understanding. Critically, its founders said there was a large amount of goodwill and trust among the various stakeholders who got it up and running.

Takeaways and First Principles

This three-part analysis—the literature review, expert insights, and global governance mapping—revealed a through line: Worsening power asymmetries are at the heart of much conflict, harm, and governance dysfunction in the digital domain. Whereas the internet emerged and spread as a relatively open, distributed enterprise, extreme concentrations of power now prevail as a handful of private companies and nation-states have consolidated control over digital technologies and spaces. Power is neither the sole nor absolute source of the world's digital troubles; the origins of any complex challenge are multidimensional. But power in and over the digital realm is more concentrated than ever before and that has created a trajectory for the digital future that imperils security, equity, and human rights.

"Power in and over the digital realm is more concentrated than ever before and that has created a trajectory for the digital future that imperils security, equity, and human rights."

First, consider corporate concentrations of power. Commentators have noted that cycles of decentralization and centralization pervade the history of the digital technology industry: Computing decentralized when the personal computer replaced mainframes, but then centralized again with Microsoft's proprietary operating system.[151] Open-source software and open protocols made for a decentralized world wide web, until Google, Meta, Amazon, and others used big data to monopolize core online services. Acquisitions and the high cost of computing hardware needed to train large language models have shifted cutting-edge AI research and development from a distributed network of university labs and startups to a handful of tech giants.[152] (It remains to be seen if Meta's decision to release the source code of its LLaMA foundation model will lead to meaningful decentralization).[153]

Today, in most areas of digital technology, centralization is at a zenith, as a combination of network effects, anti-competitive practices, and laissez-faire regulation have enabled American tech companies to become the world's largest, most influential firms and carry out policies and practices worldwide that advance corporate interest, rather than the public interest. National

governments, too, are concentrating digital power. Big data and ever-more sophisticated and pervasive surveillance technologies enable state censorship and control.

Government-ordered internet shutdowns have become more frequent, more precise, harder to detect, and longer in duration.[154] Although an American was elected to lead the ITU, the digital authoritarian model of governance is gaining ground: In its 2022 annual report, Freedom House, a pro-democracy NGO, found that internet freedom had declined worldwide for the 12th consecutive year, as "more governments than ever are exerting control over what people can access and share online by blocking foreign websites, hoarding personal data, and centralizing their countries' technical infrastructure."[155]

At the same time, the digital domain is the most active battlefield in the escalating, zero-sum power struggle between the U.S. and China. In addition to the tussle over cyber norms and technical standards playing out in multilateral fora, the U.S. and China are vying to limit the other's access to rare earth minerals and the development and spread of the other's digital technologies like 5G infrastructure, subsea internet cables, semiconductors, and cloud computing. Increasing acrimony in the politics of each country toward the other impedes cooperation on urgent global digital governance areas, such as AI risk.

This struggle affects all nations, as the great powers push less influential countries to choose a side, and it shapes the parameters of digitization for the world. Especially when it comes to AI, considerations of safety, justice, and human rights take a back seat in the rush, echoed by U.S. policymakers and commentators, to "win the AI arms race."[156]

Addressing these global power asymmetries is not simple. Since the issue is planetary in scope and born of entrenched social, political, and economic systems, it is not a problem to be solved but a situation to be managed. Though they can help, new technologies and markets are insufficient tools. It will require global governance that can diminish concentrations of power and make institutions and systems more accessible and equitable. It must at the same time maintain the decentralized, open, and democratic approaches to technological design and application that have enabled innovation and growth in the digital economy.

Global digital governance is beyond the scope of a single institution. Rather, as Anne-Marie Slaughter and Fadi Chehadé have written, it will take a networked, multi-stakeholder ecosystem able to "co-design digital norms, or actionable rules and implementation guidelines that give companies and citizens clear incentives to cooperate responsibly in the digital world."[157] Some of these will be national regulations and international treaties; some will be new multi-stakeholder bodies in the ICANN mold; some will be private sector initiatives like the Santa Clara

Principles[158] or the Frontier Model Forum; and others will be norms and habits of mind.

In our analysis, many ideas emerged about the frameworks and institutions that should be a part of this ecosystem. We identified several takeaways from across the five issue areas of study that could contribute to shaping a more equitable digital future. Below we identify five first principles that should inform future interventions and the way forward.

1. Pay It Forward to the Next Generation on AI Governance

It is not a stretch to say that the digital future depends on the global governance models and principles we build consensus on for AI. These systems are the cutting edge of digital technology, and they will have an impact on all of the issue areas examined in this report. Governance will steer the course of the technology and its outcomes. As the AI researcher Timnit Gebru and her co-authors have written, AI development "is not a preordained path where our only choice is how fast to run."[159] Global institutions are needed to bend that path toward safety, equity, and societal benefit. We have an opportunity to get in front of some of the worst possible harms stemming from AI right now, and if we do so we will be able to pay it forward to future generations when it comes to ensuring a safe, secure, and equitable digital domain.

There is no shortage of work on principles and guidelines for safe, ethical AI. Over the past several years, research labs, companies, governments, and many others have produced more than 100 sets of principles for safe, trustworthy, and ethical AI. A 2020 survey of 36 major ethical and rights-based AI principles documents found a fair amount of consensus, what the authors called a "normative core," around the themes of privacy, accountability, safety, transparency, fairness and non-discrimination, human control of technology, professional responsibility, and human values.[160] Since the release of ChatGPT, the proliferation of guidelines and calls to action have only intensified.[161]

Fewer have tackled the question of what kinds of institutions could govern the technology and facilitate global adoption of responsible AI principles and practices. A fragmented global AI governance regime exists, but only among Western democracies and their allies.[162] The main players are intergovernmental organizations, such as the OECD, G7, and the ITU's AI for Good initiative; technical and standards associations like the IEEE and ISO/IEC; companies, such as the AI giants that recently announced the Frontier Model Forum; and loose partnerships of non-state actors like the Partnership on AI. A slew of initiatives involving state and local governments, activist movements, research institutes, NGOs, and others also play a role in agenda-setting and norm-creation that indirectly influence global outcomes. Bilaterally, the EU-U.S. Trade and

Technology Council has opened discussions to harmonize the jurisdictions' emerging regulatory approaches to AI.[163]

None of these "global" efforts involve much of the globe. China is absent, as are developing nations with the exception of the OECD's three Latin American members: Chile, Colombia, and Costa Rica. Given the ease with which AI models can proliferate across borders, global governance cannot have any gaps. It must involve the two biggest national players, the U.S. and China, which is no easy task given the digital competition and acrimonious domestic politics that dim the prospects for cooperation. Nor can global governance exclude the developing economies that will not only play an ever-larger role in the digital ecosystem as they continue to develop, but who are major stakeholders today, given that the digital economy, AI workforce, and impacts of technology are all transnational.

The governance model must be multi-stakeholder, involving those in civil society, ethics, and technical communities, and especially the tech companies who are developing AI. These firms are sovereign actors with as much power as nation-states; as Ian Bremmer and Mustafa Suleyman put it, "any regulatory structure that excludes the real agents of AI power is doomed to fail."[164]

An AI global governance model would have several objectives. A team of researchers from DeepMind and a few universities identified four: spreading beneficial technology, harmonizing regulation, ensuring safe development and use, and managing geopolitical risks.[165] Several researchers, experts, and officials have proposed new international governance bodies and agencies that could carry out these objectives.

The challenge, however, is not so much conceptualizing new institutions for global governance, but overcoming the geopolitical status quo to actually create them. In the face of entrenched corporate power and the fragmentation, distrust, and competition among nations—the U.S. and China especially—what kind of process could be both inclusive and high-level enough to bring all the players to the table and facilitate the cooperation necessary to stand up new institutions?

Nearly 70 years ago, the world faced an uncertain future due to the proliferation of nuclear weapons. The Cold War was heating up, with the U.S. and Soviet Union racing to build more and more-powerful bombs. Albert Einstein and Bertrand Russell penned a manifesto calling for a global scientific conference to understand and build consensus for managing the risks posed by the novel technology. In 1957, 22 eminent scientists from the U.S., Soviet Union, China, Japan, and six other nations gathered in Pugwash, Nova Scotia.[166]

Proposed AI Global Governance Institutions

Safe Development and Use	
Type of Institution	**Inspirations**
Scientific Observatory and Research Body	Intergovernment Panel on Climate Change • Intergovernmental Science-Policy Plarform on Biodiversity and Ecosystem Services • CERN
Monitoring and Auditing Organization	International Atomic Energy Agency
Regulation Harmonization	
Type of Institution	**Inspirations**
Standard-setting and Enforcement Body	Financial Action Task Force • International Civil Aviation Organization • Christchurch Call to Action
Coordinator for International Regulations and Treatymaking	UN Environmental Programme
Geopolitical Risk Management	
Type of Institution	**Inspirations**
AI Disruptions Response Body	Financial Stability Board • Bank of International Settlements
Risk Mitigation Body	Arms Control Regime
Technology Dissemination	
Type of Institution	**Inspirations**
AI Development and Distribution Collaborative	Gavi, the Vaccine Alliance • Global Environment Facility • Belmont Forum

Source: DeepMind | Ian Bremmer and Mustafa Suleyman | Jacinda Ardern | New America

NEW AMERICA

That first meeting spawned follow-up conferences, workshops, study groups, and symposia, involving an ever-greater number of scientists, experts, and government officials attending in an unofficial capacity. Pugwash, as the platform became known, was vital for building global scientific consensus and shaping an international governance regime to manage nuclear, chemical, and biological weapons during an era of fraught or frozen relations between the Eastern Bloc and the Western democracies.[167] The institution performed essential scientific and consensus-building work that contributed to the Partial Test Ban Treaty of 1963, the Non-Proliferation Treaty of 1968, and other international agreements on weapons of mass destruction (WMD).[168] In a larger sense, Pugwash expanded global WMD governance beyond nation-states, operationalizing the idea that national sovereignty was not singular but that the greater interests of humanity also mattered. In 1995, Pugwash was awarded the Nobel Peace Prize for its contributions to WMD governance.

AI is vastly different from nuclear technology. AI proliferates easily and has countless applications, with varying levels of risk. The most powerful systems are built not by governments but by private companies. Perhaps only with the exception of autonomous military applications, the nonproliferation and control regime that has managed nuclear weapons is wholly unsuited for governing AI.

An evolved model of the Pugwash conference format could be just as effective for AI as it was for WMD. The starting point would be the recognition that AI is a planetary issue, one that affects societies worldwide, regardless of whether they own or develop the technology. Countries large and small will adopt, shape, and experience the consequences of AI systems; everyone has a stake in their safe, beneficial development and use. Thus, governance of the technology must be multi-stakeholder and globally representative, not left solely in the hands of the most powerful nations and corporations.

Just as the original Pugwash conferences made progress on WMD governance by involving scientists and experts representing non-national interests, a similar effort for AI would need to grapple with the challenge posed by not only national sovereignty, but also corporate sovereignty. Primarily, that means facilitating productive cooperation between the U.S. and China. Despite political tensions, the two countries' scientific and research communities frequently collaborate: Chinese and American AI researchers teamed up to publish more articles between 2010 and 2021 than collaborators from any two other nations.[169] And, it means building cross-sectoral consensus that can translate to regulation or other forms of pressure that can diminish corporate power and positively shape corporate behavior.

2. Invest in Distributed Access and Failsafes to Safeguard Connectivity

Concentration of power and inequality characterize various types of digital access, whether to the internet or to emerging technologies like AI models. Harmful outcomes, especially those that emerge from disparities between developing and wealthy nations, will persist so long as ownership and access are concentrated in the rich world. The absence of technology means underserved populations miss out on the benefits; the presence of technology developed by and for a different population can have unintended, dangerous consequences. Global governance should go beyond simply managing risks and harms. It should recognize that digital access is a priority for development as well as for security: Inequalities and economic disruption resulting from AI and other emerging technologies risk stoking populism and dangerous social upheaval.[170]

Despite advances in network technology, internet access is still highly centralized in ISPs. In many countries, these gatekeepers are either private monopolies or state-owned enterprises, often subject to government influence and control, which enables arbitrary shutdowns. In other countries, these gatekeepers lack the profit incentive to provide broadband or mobile service in marginalized, poor, or rural communities. They might have political clout that enables them to block competitors from entering a market.[171] The first objective laid out in the UN Secretary General's Roadmap for Digital Cooperation is to achieve universal connectivity by 2030.[172] That connectivity will only be meaningful if distributed modes of access are made available.

Multilateral development banks and agencies should increase investments in "fail-safes" that can help shift the stewardship of connectivity away from ISPs and corporate power toward a more distributed model based on various multi-stakeholder initiatives that enable multiple access points, multiple providers, and multiple modes and means to connect. Fail-safes are alternative, modularized, or redundant means of access and connectivity. The World Bank, which is administering the Digital Development Partnership involving 11 national governments and three multinational corporations, the United Nations Development Programme, and other multilateral agencies and partnerships focused on universal access should promote the development and deployment of fail-safes.

For instance, satellite internet systems are one type of fail-safe. Solar-based internet protocols mitigate the power of nation states to block or interrupt access by optimizing system designs around planetary limitations. Though the first entrants in this field are private companies such as SpaceX and Amazon, public agencies such as the European Commission are investing in satellite internet systems, and it would be easy to imagine new private-public partnerships aimed at providing affordable or free access in rural, impoverished, or conflict-affected areas.[173]

Source: Unsplash/SpaceX

Some municipalities seeking to strengthen meaningful connectivity for historically marginalized communities are taking the fail-safe approach, deploying redundant community and municipal broadband networks. In the city of Chattanooga, Tennessee, an open network called "the Gig" was built on the back of a city-owned electricity distribution system and is funded by a bond issue and a stimulus grant. The Gig charges reasonable rates for some of the fastest internet speeds on the planet and prioritizes access for low-income individuals.[174] In New York City, a community network called NYC Mesh taps into existing internet infrastructure and connects to IXPs to provide a low-cost alternative to ISPs and more coverage opportunities across the city. Volunteers operate the network, which relies on user donations to operate. These kinds of local, grassroots initiatives can provide access to historically marginalized communities or individuals disenfranchised by the prohibitive costs imposed by ISPs.

At the same time, governments, multilateral agencies, and companies should address the divide in access to emerging technologies such as AI systems by investing in mechanisms that can transfer technology, raise funding, provide technical assistance, and develop education programs for data literacy. A team of DeepMind and university researchers, for example, have proposed a public-private "Frontier AI Collaborative" that would pool funding to purchase beneficial advanced AI models and then provide access to developing countries.[175] The inspiration for the collaborative is GAVI, The Vaccine Alliance, a global public-private hub that gathers resources to purchase and then deliver vaccines to the world's poorest people.

Instead of directly transferring technology, a multi-stakeholder financing mechanism could provide grants and blended funding for specific AI or other emerging technology development projects. Such an institution might emulate features of the Global Environment Facility, the multilateral fund that finances environmental and climate change mitigation and adaptation in developing countries. A true multi-stakeholder analog is the Belmont Forum, a collaborative of funding organizations, international science councils, and regional consortia that facilitates international, transdisciplinary research to help understand, mitigate, and support adaptation to climate change. Since 2009, the Forum has disbursed hundreds of millions of euros to support 134 projects undertaken by more than 1,000 scientists hailing from 90 countries.[176] In addition to helping with financing, a digitally focused Belmont Forum could provide developing nations with publicly accessible large datasets to develop and train their own AI foundation models.

In addition, governments should create incentives to decentralize AI research and development. For instance, legislation passed by the 117th U.S. Congress designates roughly $80 billion to regional industrial policy initiatives such as the U.S. Economic Development Agency's Tech Hub investments and the National Science Foundation's Regional Innovation Engines competition.[177] Regional innovation ecosystems such as Southwestern Pennsylvania's New Economy Collaborative have received funds to supercharge their robotics and autonomous technologies sectors. This model of regional innovation hubs could be implemented globally by increasing investment outside of the U.S. in nontraditional innovation ecosystems in the developing world, which, as of now, lack the public and private investment necessary to compete with wealthy economies.

3. Privilege Regional Principles and Standards in Cybercrime

The battles playing out in multilateral fora between democracies and autocracies over the standards and norms of the digital domain illustrate the paradox at the heart of global digital governance. On the one hand, digital space is essentially borderless, and without universal standards and norms malicious actors will simply move to lenient jurisdictions. Yet, geopolitical competition and bad-faith engagement of autocracies stymie the prospects for global consensus on various cyber issues. Not only that, strict universal standards are not always desirable or practicable, given the vast differences in digitization across the world.

Regionally based institutions and coalitions of stakeholders that draw from similar legal and ethical traditions should be privileged when it comes to driving consensus on policy responses to cybercrime. At the same time, states seeking to advance global cyber norms that encourage a safe, open, equitable digital domain should try to generate consensus for widely-acceptable baseline standards on attribution, accountability, and risk management when it comes to

cyberattacks and cyber-enabled criminal acts. Even though changing the cyber behavior of autocracies may prove difficult, democracies have an opportunity to encourage non-aligned, developing countries to adopt minimum standards and norms. But in order to succeed, those democracies need to understand and respect local context and allow countries the agency to tailor digital norms to their circumstances.

Cybercrime is one area where this approach might yield results. Putting aside the fact that some states sponsor transnational cybercrime, different regions and groups experience cybercrime differently. Norms surrounding privacy and acceptable speech vary from one jurisdiction and culture to another, for instance. In addition, technical literacy and capacity determine the real and perceived harm of a cybercrime. Low-income countries might have justifiably little interest in passing cybercrime legislation when lack of broadband access or electricity are more pressing concerns for the population. These challenges dim the prospects of universal support for a comprehensive definition of cybercrime.

The Digital Futures Task Force working group on cybercrime proposed a looser global framework definition of cybercrime that distinguishes between technical cybercrimes and social cybercrimes. Democracies then could encourage regional organizations and clubs, such as ASEAN and ECOWAS (the Economic Community of West African States), to elevate the issue on their agendas and categorize cybercrime within that framework on a regional basis. The demand-side approach could encourage national governments and regional organizations to prioritize demand-side governance solutions: capacity building, victim compensation, and cyber awareness and education. As a practical matter, that might be a more promising governance approach, since, so long as autocracies continue to enable transnational cybercrime, curbing the global supply of cybercriminal activity will be a challenge.

4. Practice What You Preach on Surveillance and Spyware

Another area where democracies could do more to shape global cyber norms is in digital surveillance. The prospect of international agreements prohibiting or constraining the use of surveillance technologies in the near future appears remote, as these tools have become indispensable instruments of control for authoritarian nations. However, the U.S. and other democracies could build greater international consensus for limiting the export and use of certain harmful surveillance technologies.

One such type of technology is commercial spyware. Between 2011 and 2023, at least 74 governments hired commercial firms to acquire spyware and digital forensic technologies.[178] These technologies violate privacy rights and also threaten national security: In 2021, revelations emerged that foreign entities had used Pegasus software, a hacking tool used to spy on individuals via mobile

phone, to spy on government officials such as French President Emmanuel Macron and Pakistan's Prime Minister Imran Khan.[179]

Following a public outcry amid revelations that the U.S. Federal Bureau of Investigation had purchased the software, the U.S. blacklisted NSO, the producer of Pegasus software, nearly bankrupting it. In March 2023, the U.S. announced rules that restrict the operational use of commercial spyware that poses a risk to national security.[180] Across the Atlantic, there have been calls for the E.U. to implement a moratorium on commercial spyware.[181] In March 2023, the Biden Administration issued a joint statement with the governments of Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, and the United Kingdom on their efforts to prevent the proliferation and misuse of commercial spyware.

While these were promising steps, the U.S. has not fully implemented its own commitments. Despite its prohibition on the use of commercial spyware, the U.S. government blacklist is spotty and agencies such as the Drug Enforcement Administration continue to use spyware tools created by foreign companies.[182] The U.S. should lead by example and enact a truly government-wide moratorium on commercial spyware. Otherwise, these declarations and statements ring hollow. In doing so, the U.S. has the opportunity to shape global cyber norms and rally foreign partners to implement an international moratorium on the exportation, sale, and use of spyware. While autocratic nations are unlikely to endorse such a moratorium, there is a potential for engagement with developing, non-aligned nations that are frequently the victims of spyware, who may be inclined to adopt this norm.

5. Redistribute Data Value to Rebalance the Data Protection Equation

Central to the debate on data protection and data sovereignty is the question of ownership. Who should own the data, and therefore the value, generated by individuals? As it stands now, those who create data do not own it. In order to access most digital services, users relinquish their right to ownership per the website's terms and conditions. This is by design. The business models of several of the largest technology companies depend on big data. These companies generate vast revenues from the personal data of their product users, who provide that data freely and see no share of the value it affords. Large language models (LLMs) are the latest example of this imbalance; training an advanced LLM requires tens of gigabytes of text found on millions of websites. The creators of this text receive no compensation for its use.

The users who generate big data should have rights and be entitled to compensation for its use. One mechanism to do this could be a fund that allocates a "data dividend" to individuals. Modeled after Alaska's Permanent Fund, a state-owned corporation that issues every Alaskan an annual payment

drawn from the proceeds of the state's oil revenues, a permanent data fund would pay every resident of a jurisdiction an annual payment for the value of the data they create and that tech companies use.[183] National and even state governments should create data funds, capitalizing them with fees levied on large tech companies.[184]

Other proposals envision new guilds, unions, or public coalitions that could collectively bargain with Big Tech companies over compensation and usage rights for the data they provide.[185] Because the data of one user is virtually worthless but the data of many together is valuable, these proposals would require users to collectively organize and bargain to have any power in the data economy.[186] The responsibility of collective bargaining could be taken on by existing unions or civil society organizations that have the experience needed to negotiate with Big Tech multinationals.

Next Steps: The Future of the Digital Futures Task Force

In 2024, we plan to reconvene the Digital Futures Task Force and expand its membership to include even more participants from the developing world and a larger number of three types of experts: (1) lawyers, who understand the legal implications and constraints imposed by emergent technologies on shared conceptions of sovereignty and citizenship; (2) technologists, who understand the possibilities and limitations of emergent capabilities and utilities; and (3) ethicists, who understand the social, psychological, and moral ramifications of emergent technologies. These three disciplines—law, engineering, and ethics—are essential for developing a sociotechnical approach to digital governance.

The task force will narrow its focus to two areas where acute power asymmetries, especially between wealthy nations and developing nations, are especially consequential for the digital future.

The first is global AI governance. There are few multi-stakeholder processes aimed at creating frameworks and institutions for governing AI; even fewer include representation from much of the developing world. As an example, one international assessment seeking to inform global governance models for artificial general intelligence surveyed 55 AI leaders, not one of whom was from Africa, South Asia, or Latin America.[187] Our plan is to change the conversation by changing who is at the table talking about what is next. The task force will bring a geographically diverse set of views together to provide a better understanding of how developing nations experience AI and what their priorities are for its governance. In this way, we aim to help broaden global engagement in the AI governance conversation.

The second area the task force will address is the global battle over data protection and data access playing out in the developing world. The efforts of U.S.

and Chinese companies to control the data, eyeballs, and network infrastructure in developing countries is undermining national sovereignty and driving conflict. The EU, India, and Russia, meanwhile, are carving out their own lanes in this race for influence over how emergent technologies are governed in developing economies. A detailed, region-by-region and country-by-country picture of this frontline in global cyberpolitics is needed, especially in four areas:

- Data Sovereignty: Who is laying claim to a country's data? And how?
- Data Protection: Who is supplying a country with surveillance technologies, big data tools, and the computing resources used in security and public safety?
- Data Access: How do foreign countries and companies influence the parameters of internet access in a given country?
- Agenda Setting: Who is influencing a nation's decision-making when it comes to legislation and policy surrounding digital technologies? And how?

Big picture: The challenge we've set for ourselves is to contribute to the dispersed global effort to bring about more principled stewardship of the digital domain. The question of how to conceptualize sovereignty is the backbone of many conversations about the future of the digital domain. The struggles we are now experiencing over how to think about and define so-called Rubicon thresholds in the digital domain will have implications for the future of the open internet, cybersecurity, AI, and the balance of power in the digital domain between technopolies and nations, citizens and governments, and wealthy and developing economies. We know that global institutions and fora are bound to proliferate; that is a good thing. We need more public debate, not less, if we want to get a handle on the digital future.

Notes

1 Benjamin Hart, "The Grim New Consensus on Social Media and Teen Depression," *New York Magazine*, May 8, 2023, https://nymag.com/intelligencer/2023/05/the-grim-new-consensus-on-social-media-and-teen-depression.html.

2 Mayumi Hirosawa and Ryohei Yasoshima, "ITU G7 Backs Deep Sea Cable Network for Nations," *SubTel Forum*, https://subtelforum.com/g-7-backs-deep-sea-cable-network-for-nations/.

3 Kristen Cordell, "The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of," *Center for Strategic and International Studies Commentary* (blog), December 14, 2020, https://www.csis.org/analysis/international-telecommunication-union-most-important-un-agency-you-have-never-heard.

4 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 283.

5 John McCarthy's work and life have been memorialized by the Computer History Museum. To learn more, read McCarthy's bio here: https://computerhistory.org/profile/john-mccarthy.

6 Tim Büthe, Christian Djeffal, Christoph Lütge, Sabine Maasen, and Nora von Ingersleben-Seip, "Governing AI—Attempting to Herd Cats? Introduction to the Special Issue on the Governance of Artificial Intelligence," *Journal of European Public Policy* 29, no. 11 (November 4, 2022): 1721–1752, https://doi.org/10.1080/13501763.2022.2126515.

7 Raffaele Pugliese, Stefano Regondi, and Ricardo Marini, "Machine Learning-Based Approach: Global Trends, Research Directions, and Regulatory Standpoints," *Data Science and Management* 4 (December 2021): 19–29, https://doi.org/10.1016/j.dsm.2021.12.002.

8 Emily Aiken, Suzanne Bellue, Dean Karlan, Christopher Udry, and Joshua Blumenstock, *Machine Learning and Mobile Phone Data Can Improve the Targeting of Humanitarian Assistance* (Cambridge, MA: National Bureau of Economic Research, July 2021), https://www.nber.org/papers/w29070.

9 Faiz Siddiqui and Jeremy B. Merrill, "17 Fatalities, 736 Crashes: The Shocking Toll of Tesla's Autopilot," *Washington Post*, June 10, 2023, https://www.washingtonpost.com/technology/2023/06/10/tesla-autopilot-crashes-elon-musk/.

10 Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker, and Kate Crawford, *AI Now 2017 Report* (New York: AI Now Institute, October 18, 2017), https://ainowinstitute.org/publication/ai-now-2017-report-2.

11 For an example of gender bias, see Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018): 1–15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

12 Krystal Hu, "ChatGPT Sets Record for Fastest-Growing User Base—Analyst Note," *Reuters*, February 2, 2023, https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.

13 *Policymaking in the Pause* (Cambridge, MA: Future of Life Institute, April 12, 2023), https://futureoflife.org/wp-content/uploads/2023/04/FLI_Policymaking_In_The_Pause.pdf; *Governing AI: A Blueprint for the Future* (Redmond, WA: Microsoft, 2023), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw.

14 "Statement on AI Risk," Center for AI Safety, May 30, 2023, https://www.safe.ai/statement-on-ai-risk. See also: "An Overview of Catastrophic AI Risks," Center for AI Safety, https://www.safe.ai/ai-risk.

15 "Open Letter to News Media and Policy Makers re: Tech Experts from the Global Majority," *Free*

Press, May 8, 2023, https://www.freepress.net/sites/default/files/2023-05/global_coalition_open_letter_to_news_media_and_policymakers.pdf; Seth Lazar, Jeremy Howard, and Arvind Narayanan, "Is Avoiding Extinction from AI Really an Urgent Priority?" *AI Snake Oil* (blog), May 31, 2023, https://aisnakeoil.substack.com/p/is-avoiding-extinction-from-ai-really.

16 Blake Richards, Blaise Aguera y Arcas, Guillaume Lajoie, and Dhanya Sridhar, "The Illusion of AI's Existential Risk," *Noema*, July 18, 2023, https://www.noemamag.com/the-illusion-of-ais-existential-risk/; Kenan Malik, "Fantasy Fears about AI Are Obscuring How We Already Abuse Machine Intelligence," *Guardian*, June 11, 2023, https://www.theguardian.com/commentisfree/2023/jun/11/big-tech-warns-of-threat-from-ai-but-the-real-danger-is-the-people-behind-it.

17 Langdon Winner, "Do Artifacts Have Politics?" *Daedalus* 109, no. 1 (Winter 1980): 121–136, https://www.jstor.org/stable/20024652.

18 Nestor Maslej et al., *Artificial Intelligence Index Report 2023* (Stanford, CA: Stanford Institute for Human-Centered Artificial Intelligence, April 2023), https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf.

19 Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell, "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?" in *FAccT '21 Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (March 2021): 610–623, https://doi.org/10.1145/3442188.3445922.

20 Roxanne Heston and Remco Zwetsloot, *Mapping U.S. Multinationals' Global AI R&D Activity* (Washington, DC: Center for Security and Emerging Technology, December 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Mapping-U.S.-Multinationals-Global-AI-RD-Activity-1.pdf.

21 Liz Lindqwister, "San Francisco's Next Gold Rush Is Already Here, and You've Been Using It for Years," *San Francisco Standard*, January 23, 2023, https://sfstandard.com/2023/01/23/san-franciscos-next-gold-rush-is-already-here-and-youve-been-using-it-for-years.

22 Josh Dzieza, "AI Is a Lot of Work," *Verge*, June 20, 2023, https://www.theverge.com/features/23764584/ai-artificial-intelligence-data-notation-labor-scale-surge-remotasks-openai-chatbots.

23 Billy Perrigo, "Inside Facebook's African Sweatshop," *Time*, February 14, 2022, https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/.

24 "Generative AI Could Raise Global GDP by 7%," Goldman Sachs, April 5, 2023, https://www.goldmansachs.com/intelligence/pages/generative-ai-could-raise-global-gdp-by-7-percent.html.

25 Jacques Bughin, Jeongmin Seong, James Manyika, Michael Chui, and Raoul Joshi, *Notes from the AI Frontier: Modeling the Impact of AI on the World Economy* (Washington, DC: McKinsey Global Institute, September 4, 2018), https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-AI-frontier-modeling-the-impact-of-ai-on-the-world-economy.

26 Chinmayi Arun, "AI and the Global South: Designing for Other Worlds," in *The Oxford Handbook of Ethics of AI*, ed. Markus D. Dubber, Frank Pasquale, and Sunit Das (Oxford, UK: Oxford Academic, July 9, 2020), https://doi.org/10.1093/oxfordhb/9780190067397.013.38.

27 Adam Zable and Susan Ariel Aaronson, *For the People but Not by the People: Public Engagement in National AI Strategies* (Washington, DC: Digital Trade and Data Governance Hub at George Washington University, December 22, 2022), https://datagovhub.letsnod.com/images/DataGov-Year-2/

Special%20Report%20from%20the%20Global%20Data%20Governance%20Mapping%20Project.pdf.

28 John Villasenor, *Products Liability Law as a Way to Address AI Harms* (Washington, DC: Brookings Institution, 2019), https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/; James Guszcza, Iyad Rahwan, Will Bible, Manuel Cebrian, and Vic Katyal, "Why We Need to Audit Algorithms," *Harvard Business Review*, November 28, 2018, https://hbr.org/2018/11/why-we-need-to-audit-algorithms.

29 Internet Society, "Promoting the Internet Exchange Points (IXP) Development," December 2012, https://www.internetsociety.org/wp-content/uploads/2012/12/promote-ixp-guide.pdf; Daniel Opperman, ed., *Internet Governance in the Global South: History, Theory, and Contemporary Debates* (São Paulo, Brazil: University of São Paulo, 2008), https://www.ssoar.info/ssoar/bitstream/handle/document/65805/ssoar-2018-oppermann-Internet_Governance_in_the_Global.pdf.

30 Internet Society, *Promoting the Internet Exchange Points (IXP) Development*.

31 International Telecommunication Union, "Internet Surge Slows as Pandemic Impact Evolves," United Nations, September 16, 2022, https://www.itu.int/en/mediacentre/Pages/PR-2022-09-16-Internet-surge-slows.aspx.

32 International Telecommunication Union, "Internet Surge Slows as Pandemic Impact Evolves," https://www.itu.int/en/mediacentre/Pages/PR-2022-09-16-Internet-surge-slows.aspx.

33 Nadia Jeffrie, *The Mobile Gender Gap Report 2023* (London, UK: GSMA, 2023), https://www.gsma.com/r/gender-gap/.

34 International Telecommunication Union, "ICT Facts and Figures 2022," https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

35 "Digital Development," World Bank, March 31, 2023, https://www.worldbank.org/en/topic/digitaldevelopment/overview.

36 Paul DiMaggio and Bart Bonikowski, "Make Money Surfing the Web? The Impact of Internet Use on the Earnings of U.S. Workers," *American Sociological Review* 73, no. 2 (April 1, 2008), https://doi.org/10.1177/000312240807300203.

37 Slavka Antonova, "Digital Divide in Global Internet Governance: The 'Access' Issue Area," *Journal of Power, Politics, and Governance* 2, no. 2 (June 2014): 101–125, http://jppgnet.com/journals/jppg/Vol_2_No_2_June_2014/6.pdf.

38 Antonova, "Digital Divide in Global Internet Governance."

39 International Telecommunication Union, "Internet Surge Slows as Pandemic Impact Evolves," International Telecommunication Unions (press release), September 16, 2022, https://www.itu.int/en/mediacentre/Pages/PR-2022-09-16-Internet-surge-slows.aspx.

40 Natalia Williams, "Overview on Global Digital Divide," *Global Journal of Technology and Optimization* 2, no 1. (2022), https://www.hilarispublisher.com/open-access/overview-on-global-digital-divide-85619.html.

41 Akshit Singla, "Understanding the Impact of Social Media on Decision Making," (master's thesis, Massachusetts Institute of Technology, September 2022), https://dspace.mit.edu/bitstream/handle/1721.1/147370/singla-akshit-sm-sdm-2022-thesis.pdf.

42 Cheng Li, "Worsening Global Digital Divide as the US and China Continue Zero-Sum Competitions," *Order from Chaos* (blog), Brookings Institution, October 11, 2021, https://www.brookings.edu/blog/order-from-chaos/2021/10/11/worsening-global-digital-divide-as-the-us-and-china-continue-zero-sum-competitions/.

43 American Enterprise Institute, *China Global Investment Tracker* (Washington, DC: The American Enterprise Institute, 2023), https://www.aei.org/china-global-investment-tracker/; Aubrey Hruby, "The Digital Infrastructure Imperative in African Markets," *AfricaSourc*e (blog), Atlantic Council, April 8, 2021, https://www.atlanticcouncil.org/blogs/africasource/the-digital-infrastructure-imperative-in-african-markets/.

44 Juliet Nanfuka, *Digital Access and Economic Transformation in Africa* (New York: Institute for New Economic Thinking, March 2022), https://www.ineteconomics.org/uploads/papers/Digital-Access-Africa_Draft-Section-Nov-9_CT120222_Clean34.pdf.

45 Mayumi Hirosawa and Ryohei Yasoshima, "G-7 to Support Deep-Sea Cable Network for Emerging Nations," SubTel Forum, April 26, 2023, https://subtelforum.com/g-7-backs-deep-sea-cable-network-for-nations/.

46 Joe Brock, "U.S.-China Tech Cables: The Untold Story of How the U.S. Decided What China Could Learn," *Reuters*, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

47 "2Africa Subsea Cable Makes First Landing in Genoa, Italy," Meta Newsroom, April 2022, https://about.fb.com/news/2022/04/2africa-subsea-cable-makes-first-landing-in-genoa-italy/; Paul Lipscombe, "Google Officially Launches Equiano Subsea Cable," Datacenter Dynamics, https://www.datacenterdynamics.com/en/news/google-officially-launches-equiano-subsea-cable/.

48 Andrew Blum and Carey Baraka, "Google Meta Is Building an Underwater Cable Empire," Rest of World, October 4, 2022, https://restofworld.org/2022/google-meta-underwater-cables/.

49 Danielle Coleman, "Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws," *Michigan Journal of Race and Law* 24 (2019): 417–439, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1294&context=mjrl.

50 Lee Bygrave, "Privacy and Data Protection in an International Perspective," *Scandinavian Studies in Law* 56 (2011): 139–164, https://www.scandinavianlaw.se/pdf/56-8.pdf.

51 Privacy International, *Data Protection, Explained* (London, UK: Privacy International, 2018), https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf.

52 GDPR.EU, "What is GDPR? A Guide to the General Data Protection Regulation," European Union, https://gdpr.eu/what-is-gdpr/.

53 Agustín Rossi, "How the Snowden Revelations Saved the EU General Data Protection Regulation," *International Spectator* 53, no. 4 (2018): 95–111, https://doi.org/10.1080/03932729.2018.1532705.

54 Marie Baezner and Robin Patrice, "Cyber Sovereignty and Data Sovereignty," *CSS CyberDefense Trend Analysis* 2, no. 2 (2018), https://doi.org/ 10.3929/ethz-b-000314613.

55 Anita Gurumurthy and Nandini Chami, *Beyond Data Bodies: New Directions for a Feminist Theory of Data Sovereignty* (Bengaluru, India: IT for Change, January 17, 2022), https://ssrn.com/abstract=4037321.

56 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (London, U.K.: Profile Books, 2019), 360–363.

57 Dennis Broeders, Fabio Cristiano, and Monika Kaminska, "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions," *JCMS: Journal of Common Market Studies* (2023), https://doi.org/10.1111/jcms.13462.

58 Cynthia O'Donoghue et al., "Third Time's a Charm: European Commission Adopts EU-U.S. Data Privacy Framework," Reed Smith's Technology Law Dispatch, July 12, 2023. https://www.technologylawdispatch.com/2023/07/privacy-data-protection/third-times-a-charm-european-commission-adopts-eu-u-s-data-privacy-framework/.

59 Natasha Lomas, "Europe Adopts US Data Adequacy Decision," TechCrunch, July 10, 2023, https://techcrunch.com/2023/07/10/eu-us-data-privacy-framework-adoption/.

60 Karthik Nachiappan, "The International Politics of Data: When Control Trumps Protection," *Raisina Debates* (blog), Observer Research Foundation, October 26, 2022, https://www.orfonline.org/expert-speak/the-international-politics-of-data/.

61 Sammy Fang and Han Liang, "China's Emerging Data Protection Laws Bring Challenges for Conducting Investigations in China," *DLA Piper*, July 24, 2022, https://www.dlapiper.com/en/insights/publications/2022/07/chinas-emerging-data-protection-laws-bring-challenges-for-conducting-investigations-in-china.

62 Susan Ariel Aaronson, *Data is Disruptive: How Data Sovereignty is Challenging Data Governance* (Singapore: Hinrich Foundation, August 2021), https://www.wita.org/wp-content/uploads/2021/08/Data-is-disruptive-Hinrich-Foundation-white-paper-Susan-Aaronson-August-2021.pdf.

63 Julia Clark, Anna Diofasi, and Claire Casher, "850 Million People Globally Don't Have ID: Why It Matters and What We Can Do About," *Digital Development* (blog), World Bank, February 6, 2023, https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about.

64 Rahul Verma and Shantanu Kulshrestha, *Democratizing the Digital Space: Harnessing Technology to Amplify Participation in Governance Processes in the Global South* (New York: UNDP, June 29, 2022), https://southernvoice.org/wp-content/uploads/2022/06/Digital20Democracy.pdf.

65 Nannie Sköld, "UNHCR Strengthens Efforts on Digital Identity for Refugees with Estonian Support," UNHCR: Nordic and Baltic Countries, June 12, 2021, https://www.unhcr.org/neu/70493-unhcr-strengthens-efforts-on-digital-identity-for-refugees-with-estonian-support.html.

66 Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises," *Social Media + Society* 5 (July–September 2019): 1–13, https://journals.sagepub.com/doi/10.1177/2056305119863146.

67 Madianou, "Technocolonialism," https://journals.sagepub.com/doi/10.1177/2056305119863146.

68 Madianou, "Technocolonialism," https://journals.sagepub.com/doi/10.1177/2056305119863146.

69 David Lyon, *Surveillance Studies: An Overview* (Malden, MA: Polity Press, 2007), 14.

70 Thomas Mathiesen, "The Viewer Society: Michel Foucault's 'Panopticon' Revisited," *Theoretical Criminology* 8, no. 1 (1997): 215–234, https://doi.org/10.1177/1362480697001002000.

71 Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage," *British Journal of Sociology* 51, no. 4 (2000): 605–622, https://doi.org/10.1080/00071310020015280.

72 For further reading, see Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Pantheon Books, 1977), 203.

73 Christina Larson, "Who Needs Democracy When You Have Data?" *MIT Technology Review*, August 20, 2018, https://www.technologyreview.com/2018/08/20/240293/who-needs-democracy-when-you-have-data/.

74 Office of the Director of National Intelligence, *An nual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities* (Washington, DC: Office of the Director of National Intelligence, April 2022), https://www.intelligence.gov/assets/documents/702%20Documents/statistical-transparency-report/2022_IC_Annual_Statistical_Transparency_Report_cy2021.pdf.

75 Dell Cameron, "The US Is Openly Stockpiling Dirt on All Its Citizens," *Wired*, June 12, 2023, https://www.wired.com/story/odni-commercially-available-information-report/.

76 Rachel Levinson-Waldman, Harsha Panduranga, and Faiza Patel, *Social Media Surveillance by the U.S. Government* (New York: Brennan Center for Justice, January 7, 2022), www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

77 Zuboff, *The Age of Surveillance Capitalism*, 14–15.

78 Zuboff, *The Age of Surveillance Capitalism*, 8.

79 Siva Vaidhyanathan, *The Googlization of Everything (And Why We Should Worry)* (Berkeley: University of California Press, 2011), 98–107.

80 Zuboff, *The Age of Surveillance Capitalism*, 353.

81 For details on that exploit and more during the early years of networked digital tech, see: Hugo Cornwall, *The Hacker's Handbook* (London, UK: Century Communications Ltd., 1985), https://archive.org/stream/TheHackersHandbook/The%20hackers%27%20handbook_djvu.txt.

82 Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, CA: Praeger, 2010), 16.

83 Jonathan Lusthaus, "How Organized Is Organized Cybercrime?" *Global Crime* 14, no. 1 (2013), https://doi.org/10.1080/17440572.2012.759508.

84 Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," *Cybercrime Magazine*, November 13, 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

85 Geoff Blaine, "Tipping Point: SonicWall Exposes Soaring Threat Levels, Historic Power Shifts in New Report," *SonicWall* (blog), March 16, 2021, https://blog.sonicwall.com/en-us/2021/03/sonicwall-exposes-soaring-threats-historic-power-shifts-in-new-report/; David Braue, "Global Ransomware Damage Costs Predicted to Exceed $265 billion by 2031," *Cybercrime Magazine*, June 2, 2022, https://cybersecurityventures.com/ransomware-market-report-2022/.

86 "Cybersecurity Advisory: 2021 Trends Show Increased Globalized Threat of Ransomware," *U.S. Cybersecurity and Infrastructure Security Agency*, February 10, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a.

87 David E. Sanger, Clifford Krauss, and Nicole Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *New York Times*, May 8, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

88 Ravinder Barn and Balbir Barn, "An Ontological Representation of a Taxonomy for Cybercrime," in *Proceedings of the 24th European Conference on Information Systems (ECIS 2016),* Istanbul, Turkey, June 2016, http://aisel.aisnet.org/ecis2016_rp/45.

89 Douglas Thomas and Brian Loader, "Introduction-Cybercrime: Law Enforcement, Security and Surveillance in the Information Age," in *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, ed. Douglas Thomas and Brian Loader (London, UK: Routledge, 2000).

90 Sarah Gordon and Richard Ford, "On the Definition and Classification of Cybercrime," *Journal in Computer Virology* 2 (2006): 13–20, 10.1007/s11416-006-0015-z.

91 Susan W. Brenner, "Cybercrime: Re-thinking Crime Control Strategies," in *Crime Online*, ed. Yvonne Jewkes (Cullompton, U.K.: Willan Publishing, 2007), 12–28.

92 Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary Aiken, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies," *Forensic Sciences* 2, no. 2 (2002): 379–398, https://doi.org/10.3390/forensicsci2020028.

93 *Convention on Cybercrime: Special Edition Dedicated to the Drafters of the Convention (1997–2001)* (Strasbourg, France: Council on Europe, March 2022), https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e.

94 Alexander Seger, "India and the Budapest Convention: Why Not?" *Digital Frontiers* (blog), Observer Research Foundation, October 20, 2016, https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/.

95 Mercedes Page, "The Hypocrisy of Russia's Push for a New Global Cybercrime Treaty," *The Interpreter* (blog), Lowy Institute, March 7, 2022, https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

96 74th session of UN General Assembly, "Countering the Use of Information and Communications Technologies for Criminal Purposes: Report of the Third Committee," United Nations, November 25, 2019, https://digitallibrary.un.org/record/3837326.

97 "Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online," *Association for Progressive Communications*, November 6, 2019, https://www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf.

98 Mercedes Page, "The Election for the Future of the Internet," *The Interpreter* (blog), Lowy Institute, February 24, 2022, https://www.lowyinstitute.org/the-interpreter/election-future-internet.

99 Richard Barbrook and Andy Cameron, "The Californian Ideology," *Science as Culture* 6, no. 1 (January 1996): 44–72, https://doi.org/10.1080/09505439609526455.

100 Rebecca Klar, "Schumer Tees Up Senate Plan for AI Regulation," *The Hill*, June 21, 2023, https://thehill.com/policy/technology/4060343-schumer-tees-up-senate-plan-for-ai-regulation/.

101 Andrew Folks, "US State Privacy Legislation Tracker," *International Association of Privacy Professionals*, Last updated September 15, 2023, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

102 Noah Berman, Lindsay Maizland, and Andrew Chatzky, "Is China's Huawei a Threat to U.S. National Security?" *Backgrounder* (blog), Council on Foreign Relations, February 8, 2023, https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security.

103 Adi Robertson, "TikTok is Now Banned in Montana," *Verge,* May 17, 2023, https://www.theverge.com/2023/5/17/23686294/montana-tiktok-ban-signed-governor-gianforte-court.

104 William Schwartz, "The EU's Digital Services Act Confronts Silicon Valley," Wilson Center, February 15, 2023, https://www.wilsoncenter.org/article/eus-digital-services-act-confronts-silicon-valley.

105 Anu Bradford, *The Brussels Effect* (New York: Oxford University Press, 2020); Andrea Calderaro and Stella Blumfelde,"Artificial Intelligence and EU Security: The False Promise of Digital Sovereignty,"

European Security 31, no. 3 (September 2022): 415–434, https://doi.org/10.1080/09662839.2022.2101885.

106 Eliska Pirkova, "The Digital Services Act: Your Guide to the EU's New Content Moderation Rules," Access Now, July 6, 2022, updated March 17, 2023, https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/.

107 "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts," April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

108 Jaron Lanier, "There Is No AI," *New Yorker*, April 20, 2023, https://www.newyorker.com/science/annals-of-artificial-intelligence/there-is-no-ai.

109 Alex Engler, *The EU and U.S. Diverge on AI Regulation: A Transatlantic Comparison and Steps to Alignment* (Washington, DC: Brookings Institution, April 25, 2023), https://www.brookings.edu/research/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/.

110 Tate Ryan-Mosley, "Five Big Takeaways from Europe's AI Act," *MIT Technology Review*, June 19, 2023, https://www.technologyreview.com/2023/06/19/1075063/five-big-takeaways-from-europes-ai-act/.

111 Sven Smit, Magnus Tyreman, Jan Mischke, Philipp Ernst, Eric Hazan, Jurica Novak, Solveigh Hieronimus, and Guillaume Dagorret, *Securing Europe's Competitiveness: Addressing Its Technology Gap* (Washington, DC: McKinsey Global Institute, 2022), https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/securing-europes-competitiveness-addressing-its-technology-gap.

112 State Council Information Office of People's Public of China (SCIO), "The Internet in China," *China Daily*, June 8, 2010, http://www.chinadaily.com.cn/cndy/2010-06/09/content_9952206.html.

113 Paul Triolo, Samm Sacks, Graham Webster, and Rogier Creemers, "China's Cybersecurity Law One Year On," *Cybersecurity Initiative* (blog), New America, November 30, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.

114 *China: Freedom on the Net 2021* (Washington, DC: Freedom House, 2022), https://freedomhouse.org/country/china/freedom-net/2021.

115 Yaqiu Wang, "In China, the 'Great Firewall' Is Changing a Generation," *Politico Magazine*, September 1, 2020, https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385.

116 *China: Freedom on the Net 2021* (Washington, DC: Freedom House, 2022), https://freedomhouse.org/country/china/freedom-net/2021.

117 Josh Chin and Liza Lin, *Surveillance State: Inside China's Quest to Launch a New Era of Social Control* (New York: St. Martin's Press, 2022).

118 Chang Che and Jeremy Goldkorn, "China's 'Big Tech Crackdown': A Guide," *The China Project*, August 2, 2021, https://thechinaproject.com/2021/08/02/chinas-big-tech-crackdown-a-guide/.

119 Rogier Creemers, "Is China's Tech 'Crackdown' or 'Rectification' Over?" *DigiChina* (blog), Stanford University, January 25, 2023, https://digichina.stanford.edu/work/is-chinas-tech-crackdown-or-rectification-over/.

120 Xinchuchu Gao, "Sovereignty and Cyberspace: China's Ambition to Shape Cyber Norms," *China Dialogues* (blog), London School of Economics, August 18, 2022, https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/.

121 Jon Bateman, "Denying Support for Chinese and China-Enabled Authoritarianism and Repression," in *U.S.-China Technological "Decoupling": A Strategy and Policy Framework*, ed. Jon Bateman (Washington, DC: Carnegie Endowment for International Peace, 2022), https://carnegieendowment.org/2022/04/25/denying-support-for-chinese-and-china-enabled-authoritarianism-and-repression-pub-86924.

122 D. K. Srivastava, "How Digital Transformation Will Help India Accelerate Its Growth in Coming Years," *EY*, April 25, 2023, https://www.ey.com/en_in/tax/economy-watch/how-digital-transformation-will-help-india-accelerate-its-growth-in-the-coming-years.

123 India Stack, https://indiastack.org.

124 Unique Identification Authority of India, "Welcome to AADHAAR Dashboard," Government of India, https://uidai.gov.in/aadhaar_dashboard/index.php.

125 Parijat Ghosh, Navneet Chahal, Vishesh Shrivastav, and Arushi Mangla, *e-Conomy India 2023* (Boston, MA: Bain & Company, June 6, 2023), https://www.bain.com/insights/e-conomy-india-2023/.

126 Open Network for Digital Commerce, https://ondc.org/.

127 Stephen Weymouth, *India's Personal Data Protection Act and the Politics of Digital Governance* (Washington, DC: Atlantic Council, March 2023), https://www.atlanticcouncil.org/wp-content/uploads/2023/05/Indias_Data_Protection_Act.pdf.

128 Zach Rosson, Felicia Anthonio, and Carolyn Tackett, *Weapons of Control, Shields of Impunity* (New York: Access Now, February 28, 2023), https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf.

129 International Telecommunication Union, "About International Telecommunication Union," International Telecommunication Union, https://www.itu.int/en/about/Pages/default.aspx.

130 Stacie Hoffmann, Dominique Lazanski, and Emily Taylor, "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet," *Journal of Cyber Policy* 5, no. 2 (2020): 239–264, https://doi.org/10.1080/23738871.2020.1805482.

131 Mark Scott and Clothilde Goujard, "Digital Great Game: The West's Standoff Against China and Russia," *Politico*, September 8, 2022, https://www.politico.eu/article/itu-global-standard-china-russia-tech/.

132 Hoffmann, Lazanski, and Taylor, "Standardising the Splinternet."

133 Scott and Goujard, "Digital Great Game."

134 Jeffrey Ding, Paul Triolo, and Samm Sacks, "Chinese Interests Take a Big Seat at the AI Governance Table," *Cybersecurity Initiative* (blog), New America, June 20, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.

135 "Open Letter to UN General Assembly: Proposed International Convention on Cybercrime."

136 George Glover, "Big Tech Stocks' Massive Gains This Year Have Made Them Even More Dominant. That Could Be Bad News for Investors," *Markets Insider*, May 29, 2023, https://markets.businessinsider.com/news/stocks/big-tech-stocks-apple-microsoft-alphabet-amazon-nvidia-meta-charts-2023-5.

137 Omri Wallach, "The World's Tech Giants, Compared to the Size of Economies," Visual Capitalist, July 7, 2021, https://www.visualcapitalist.com/the-tech-giants-worth-compared-economies-countries/.

138 "Meta Reports Second Quarter 2023 Reports," Meta, July 26, 2023, https://s21.q4cdn.com/399680738/files/doc_news/Meta-Reports-Second-Quarter-2023-Results-2023.pdf; Daniel Ruby, "WhatsApp Statistics 2023 (User Insights and Facts)," Demand Sage, July 20, 2023, https://www.demandsage.com/whatsapp-statistics/; Daniel Ruby, "77 Instagram Statistics 2023 (Active Users and Trends)," Demand Sage, July 11, 2023, https://www.demandsage.com/instagram-statistics/.

139 Daniel Ruby, "20 Android Statistics in 2023 (Market Share & Users)," Demand Sage, April 17, 2023, https://www.demandsage.com/android-statistics/.

140 Daniel Ruby, "YouTube Statistics-Insights and Infographics," Demand Sage, June 6, 2023, https://www.demandsage.com/youtube-stats/.

141 "Search Engine Market Share: Who's Leading the Race in 2023," Kinsta, https://kinsta.com/search-engine-market-share/; "How Many People Use Google in 2023? (Users Statistics)," WPDev Shed, July 18, 2023, https://wpdevshed.com/how-many-people-use-google.

142 Ian Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order," *Foreign Affairs* 100, no. 6 (2021), https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order.

143 Jon Porter, "Whistleblowers Claim Facebook's Chaotic Australia News Ban Was a Negotiating Tactic," *Verge,* May 6, 2022, https://www.theverge.com/2022/5/6/23059684/facebook-australia-news-ban-internally-praised-overbroad-nonprofits-government-organizations.

144 Bremmer, "The Technopolar Moment"; Alexis Wichowski, "Net States Rule the World; We Need to Recognize Their Power," *Wired*, November 4, 2017, https://www.wired.com/story/net-states-rule-the-world-we-need-to-recognize-their-power/.

145 Anupam Chander, "Section 230 and the International Law of Facebook," *Yale Journal of Law & Technology* 24 (2022): 393–420, https://yjolt.org/sites/default/files/2_-_chander_-_section_230_and_the_international_law_of_facebook_0.pdf.

146 Kaamil Ahmed, "Rohingya Crisis—Plight of Myanmar's Displaced People Explained in 30 Seconds," *Guardian*, August 25, 2022,https://www.theguardian.com/world/2022/aug/25/myanmar-rohingya-people-crisis-refugees-explained-in-30-seconds.

147 Global Commission on Internet Governance, *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance* (Ontario, Canada: CIGI and Chatham House, November 2016), https://www.cigionline.org/publications/who-runs-internet-global-multi-stakeholder-model-internet-governance/.

148 United States Department of Commerce, National Telecommunications and Information Administration, "Improvement of Technical Management of Internet Names and Addresses; Proposed Rule," *Federal Register* 63, no. 34 (February 20, 1998), https://ntia.gov/federal-register-notice/improvement-technical-management-internet-names-and-addresses-proposed-rule.

149 Cecilia Testart, *Understanding ICANN's Complexity in a Growing and Changing Internet* (Cambridge, MA: Explorations in Cyber International Relations, 2014), https://ecir.mit.edu/sites/default/files/documents/%5BTestart%5D%20Understanding%20ICANN%27s%20complexity%20in%20a%20growing%20and%20changing%20Internet.pdf.

150 Internet Corporation for Assigned Names and Numbers "Developing Policy at ICANN," https://www.icann.org/policy.

151 Tim O'Reilly, "Why It's Too Early to Get Excited about Web3," *O'Reilly Media*, December 13, 2021,

https://www.oreilly.com/radar/why-its-too-early-to-get-excited-about-web3/; Steve Lohr, "At Tech's Leading Edge, Worry About a Concentration of Power," *New York Times*, September 26, 2019, https://www.nytimes.com/2019/09/26/technology/ai-computer-expense.html.

152 O'Reilly, "Why It's Too Early to Get Excited about Web3"; Lohr, "At Tech's Leading Edge."

153 Cade Metz and Mike Isaac, "In Battle Over A.I., Meta Decides to Give Away Its Crown Jewels," *New York Times*, May 18, 2023, https://www.nytimes.com/2023/05/18/technology/ai-meta-open-source.html.

154 Steven Feldstein, *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?* (Washington, DC: Carnegie Endowment for International Peace, March 31, 2022), https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687.

155 *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet* (Washington, DC: Freedom House, October 2022), https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.

156 Justin Sherman, *Reframing the U.S.-China AI 'Arms Race'* (Washington, DC: New America, March 6, 2019), https://www.newamerica.org/cybersecurity-initiative/reports/essay-reframing-the-us-china-ai-arms-race/.

157 Anne-Marie Slaughter and Fadi Chehadé, "AI's Pugwash Moment," July 24, 2023, *Project Syndicate*, https://www.project-syndicate.org/commentary/institutions-to-govern-artificial-intelligence-new-pugwash-movement-by-anne-marie-slaughter-and-fadi-chehade-2023-07.

158 *The Santa Clara Principles on Transparency and Accountability in Content Moderation*, https://santaclaraprinciples.org/.

159 Timnit Gebru, Emily M. Bender, Angelina McMillan-Major, and Margaret Mitchell, "Statement from the Listed Authors of Stochastic Parrots on the 'AI Pause' Letter," DAIR Institute, March 31, 2023, https://www.dair-institute.org/blog/letter-statement-March2023/.

160 Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, and Madhulika Srikumar, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI* (Cambridge, MA: Berkman Klein Center for Internet & Society, January 2020), http://dx.doi.org/10.2139/ssrn.3518482.

161 *The Presidio Recommendations on Responsible Generative AI* (Geneva, Switzerland: World Economic Forum, June 2023), https://www3.weforum.org/docs/WEF_Presidio_Recommendations_on_Responsible_Generative_AI_2023.pdf.

162 Lewin Schmitt, "Mapping Global AI Governance: A Nascent Regime in a Fragmented Landscape," *AI and Ethics* 2 (2022): 303–314, https://doi.org/10.1007/s43681-021-00083-y.

163 Alex Engler, *The EU and U.S. Diverge on AI Regulation: A Transatlantic Comparison and Steps to Alignment* (Washington, DC: Brookings Institution, April 25, 2023), https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/.

164 Ian Bremmer and Mustafa Suleyman, "The AI Power Paradox," *Foreign Affairs*, August 16, 2023, https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox.

165 Lewis Ho et al., "International Institutions for Advanced AI," DeepMind, July 11, 2023, https://arxiv.org/pdf/2307.04699.pdf.

166 For background and more information, see the website for the Pugwash Conferences on Science and Global Affairs: https://pugwash.org/.

167 Alison Kraft and Carola Sachse, "The Pugwash Conferences on Science and World Affairs: Vision, Rhetoric, Realities," in *Science, (Anti-)Communism and Diplomacy: The Pugwash Conferences on Science and World Affairs in the Early Cold War*, ed. Alison Kraft and Carola Sachse (Boston, MA: Brill, 2020), 1–39, https://doi.org/10.1163/9789004340176_002.

168 "Pugwash Conferences on Science and World Affairs: Facts," Nobel Prize, https://www.nobelprize.org/prizes/peace/1995/pugwash/facts.

169 Edmund L. Andrews, "China and the United States: Unlikely Partners in AI," Stanford University Human-Centered Artificial Intelligence, March 16, 2022, https://hai.stanford.edu/news/china-and-united-states-unlikely-partners-ai; Cameron F. Kerry, Joshua P. Meltzer, and Matt Sheehan, *Can Democracies Cooperate with China on AI Research?* (Washington, DC: Brookings Institution, January 2023), https://www.brookings.edu/wp-content/uploads/2023/01/Can-democracies-cooperate-with-China-on-AI-research.pdf.

170 Kyle Hiebert, "Tech-Fuelled Inequality Could Catalyze Populism 2.0," *Centre for International Governance Innovation*, October 19, 2022, https://www.cigionline.org/articles/tech-fuelled-inequality-could-catalyze-populism-20/.

171 Bill Snyder and Chris Witteman, "The Anti-Competitive Forces that Foil Speedy, Affordable Broadband," *Fast Company*, March 29, 2019, https://www.fastcompany.com/90319916/the-anti-competitive-forces-that-foil-speedy-affordable-broadband.

172 UN General Assembly, "Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation: Report of the Secretary-General," 74th session, May 29, 2020, https://www.un.org/en/content/digital-cooperation-roadmap.

173 European Commission, "Satellite Broadband," https://digital-strategy.ec.europa.eu/en/policies/satellite-broadband.

174 Ben Tarnoff, *Internet for the People* (New York: Verso, 2022), 41–42.

175 Ho et al., "International Institutions for Advanced AI," https://arxiv.org/pdf/2307.04699.pdf.

176 Belmont Forum, *Annual Report 2022* (Montevideo, Uruguay: Belmont Forum, 2022), https://www.belmontforum.org/wp-content/uploads/2023/05/Belmont-Forum-Annual-Report-2022_final-version.pdf.

177 Mark Muro, Julian Jacobs, and Sifan Liu, *Building AI Cities: How to Spread the Benefits of an Emerging Technology Across More of America* (Washington, DC: Brookings Institution, July 20, 2023), https://www.brookings.edu/articles/building-ai-cities-how-to-spread-the-benefits-of-an-emerging-technology-across-more-of-america/.

178 Steven Feldstein and Brian (Chun Hey) Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses* (Washington, DC: Carnegie Endowment for International Peace, March 14, 2023), https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

179 Sabrina Tavernise (host), "The U.S. Banned Spyware — and Then Kept Trying to Use It," *The Daily* (podcast), May 15, 2023, https://www.nytimes.com/2023/05/15/podcasts/the-daily/banning-spywear.html.

180 "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security," The White House, March 27, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-

commercial-spyware-that-poses-risks-to-national-security/; Sabrina Tavernise (host), "The U.S. Banned Spyware — and Then Kept Trying to Use It," *The Daily* (podcast), May 15, 2023, https://www.nytimes.com/2023/05/15/podcasts/the-daily/banning-spywear.html.

181 "EU Final Vote on Spyware Inquiry Must Lead to Stronger Regulation," Amnesty International, June 15, 2023, https://www.amnesty.org/en/latest/news/2023/06/eu-final-vote-on-spyware-inquiry-must-lead-to-stronger-regulation/.

182 Mark Mazzetti, Ronen Bergman, and Matina Stevis-Gridneff, "How the Global Spyware Industry Spiraled Out of Control," *New York Times*, December 8, 2022, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

183 Angel Au-Yeung, "California Wants To Copy Alaska And Pay People A 'Data Dividend,' Is It Realistic?" *Forbes*, February 14, 2019, https://www.forbes.com/sites/angelauyeung/2019/02/14/california-wants-to-copy-alaska-and-pay-people-a-data-dividend--is-it-realistic/.

184 Barath Raghavan and Bruce Schneier, "Artificial Intelligence Can't Work Without Our Data," *Politico Magazine*, June 29, 2023, https://www.politico.com/news/magazine/2023/06/29/ai-pay-americans-data-00103648.

185 Matt Prewitt, "A View of the Future of Our Data," *Noema Magazine*, February 23, 2021, https://www.noemamag.com/a-view-of-the-future-of-our-data.

186 Jaron Lanier, "There Is No AI," *New Yorker*, April 20, 2023, https://www.newyorker.com/science/annals-of-artificial-intelligence/there-is-no-ai.

187 "Transition from Artificial Narrow Intelligence to Artificial General Intelligence," The Millenium Project, April 12, 2021, https://www.millennium-project.org/transition-from-artificial-narrow-to-artificial-general-intelligence-governance.

NEW AMERICA