Global TechnoPoltics Forum

DATA:
GOVERNANCE AND GEOPOLITICS

Dec 2020

Gregory F Treverton
Pari Esfandiari

DATA:
GOVERNANCE AND GEOPOLITICS

Gregory F Treverton and Pari Esfandiari

www.TechnoPoltics.org,
ISBN: 978-1-7362034-0-8
Dec 2020

GLOBAL TECHNOPOLITICS FORUM

The conclusions and recommendations of any Global TechnoPolitics Forum publication are solely those of its authors and do not reflect the views of the Forum, its management, board of advisors, donors, or scholars.

This report is written and published in accordance with the Global TechnoPolitics Forum Policy on Intellectual Independence.

The Global TechnoPolitics Forum is a (501C) (3) nonprofit educational organization with a mission to **shape the public debate and facilitate global coordination at the intersection of technology and geopolitics.** It achieves this mission through: convenings, research, and community building.

ACKNOWLEDGEMENTS

A shorter version of this article was published in the Atlantic Council GeoTech Center Cues series earlier this year.[1]

The authors would like to thank Daniel Vale and Carmen Santiago-Urbauer of the Global TechnoPolitics Forum, Rui Daniel of the University of Southern California, and Stewart Scott at the Atlantic Council for their contributions.

Cover art credit: *On White II*, by *Wassily Kandinsky*, 1923. Abstract Art _playing the endless guessing game of interpretation.

Copyrights: © *2020 The Global TechnoPolitics Forum. All rights reserved.* No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global TechnoPolitics Forum, except in the case of brief quotations in news articles, critical articles, or reviews.

Please direct inquiries to: Global TechnoPolitics Forum: info@technopolitics.org

[1] Gregory F Treverton and Pari Esfandiari, "Why data governance matters: Use, trade, intellectual property, and diplomacy," *Atlantic Council*, September 15, 2020, https://www.atlanticcouncil.org/blogs/geotech-cues/why-data-governance-matters/.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Data is often called the black gold of the twenty-first century, and while it is different in nature, it is just as critical when it comes to geopolitics, economy, and society, a fact tragically underscored by the lack of data on testing and tracking during the pandemic. To boot, the pandemic may spawn a "9/11 moment," in which people are scared and prepared to trade their privacy for increased security—this time in health.

Data is information, and big data is often seen as simply lots of data. Thus data, information, and big data overlap, and so too do the issues involved in governing them, ranging from the seemingly prosaic (in what country will data centers be located?) to questions bearing on the nature of democracy itself (how will false news and hate speech be policed, and by whom?). To the extent that data is governed, that governance is a fractal of how the internet is governed—scattered, bottom-up, and driven by loose coordination among many actors, most of them in the private sector. As governments begin to recognize the growing significance of data, the way data is collected, stored, protected, accessed, used, and transferred over national borders is becoming a geopolitical issue.

Any discussion of data governance inevitably must confront the differences in ideological visions of the internet and fundamental cultural values that divide countries and influence their policies. Moreover, issues in governing the digital domain overlap, cut across policy areas, and even conflict. The Organization for Economic Cooperation and Development (OECD) sets out three policy goals for the digital economy: "(1) enabling the internet; (2) boosting or preserving competition within and outside the internet; and (3) protecting privacy and consumers."[2] Needless to say, those goals may conflict.

The current status and prospects of governing data might be thought of along several lines of activity, which are interrelated, but which, for the sake of clarity and with some danger of oversimplification, are discussed in the following slices: legislating privacy and data use, regulating content, using antitrust laws to dilute data monopolies, self-regulation by the tech giants, regulating digital trade, addressing

[2] Isabell Koske et al., "The Internet Economy - Regulatory Challenges and Practices," *OECD Economics Department Working Papers*, No. 1171, OECD Publishing, Paris, 2014, http://dx.doi.org/10.1787/5jxszm7x2qmr-en.

intellectual property rights (IPR) infringement, assuring cybersecurity, and practicing cyber diplomacy.

Looking across these slices makes clear that the assemblage of laws, treaties, agreements, regulations, and self-regulation today, as analysts Quest and Charrie put it, "lack transparency and coherence: The combination drives up the cost of innovation and doesn't go far enough to encourage healthy competition or to protect the billions of people worldwide who now rely on the products and services tech companies produce."[3]

As this study illustrates, the digital age presents geopolitical and philosophical problems with complexity and speed beyond the capability of the existing global architecture and its institutions. We are addressing twenty-first-century problems with a twentieth-century mindset, approach, and toolkit that are all inadequate for dealing with the cross-border, complex, opaque nature of big data and cyberspace. This worrisome geopolitical context calls for an urgent Bretton Woods-style gathering to ensure that the most transformative technologies of our time do not spiral out of control into a world order we will come to regret.

The Digital-20 (D-20) is a new initiative launched by the Global TechnoPolitics Forum aiming to fill this void and to function as a bridge between the existing global architecture and the new geopolitical context. The D-20 would build upon the important work and initiatives led by the Bretton Woods institutions, the founding internet organizations, and other think tanks in establishing international codes and standards as well as demonstrating leadership. Still in its infancy, D-20 in many respects is modeled after the G-20, with the new group broadening the scope of dialogue to new stakeholders and digitally mature ecosystems as well as shifting the focus to the key geopolitical challenges caused by emerging digital technologies. As an autonomous group with no executive power and no binding decisions, its primary impact lies in creating trust and peer-to-peer intimacy among members as they develop a shared diagnosis of potential problems and a common analytical framework in small, intimate convenings. Building on this trust, D-20 will strive to produce actionable and measurable outcomes.

[3] Lisa Quest and Anthony Charrie, "The Right Way to Regulate the Tech Industry," *MIT Sloan Management Review*, September 19, 2019, https://sloanreview.mit.edu/article/the-right-way-to-regulate-the-tech-industry/.

INTRODUCTION

If oil was the black gold of the twentieth century, big data, while fundamentally different in nature, has taken up that label in the twenty-first.[4] The COVID-19 pandemic has driven home, tragically, just how valuable big data is. A lack of data on early testing and contact tracing caused tens of thousands of people to die needlessly, as well as the United States and other nations to shutter their economies. The pandemic and its aftermath threaten to make data all the more important and geopolitical, compounding the challenges of governing it. The pandemic began with a lack of data, followed by cybercrime and, more cynical, espionage aimed at data integrity. Unsurprisingly, a full geopolitical blame game followed. Finally, the waves of the pandemic seem almost certain to spawn another "9/11 moment," in which scared citizens are prepared to exchange their privacy for greater security—this time under the guise of health security. As economies reopen, plans to prevent new spikes in COVID-19 are emerging, each with distinct strategies and priorities. Nevertheless, all approaches acknowledge the fundamental role data will hold—personal data, healthcare data, commercial data, telecommunications data, and security data, in particular.

Data may resemble oil in importance but is fundamentally different. Oil was a commodity that gained value through scarcity. Data on the other hand, gains value as it becomes big, connected, and dynamic. Oil was somewhere, but data is everywhere. Oil needed the infrastructure of ships and pipelines to derive market value. Data requires infrastructure too, but the scale of that infrastructure, relative to the market value of data itself, is much smaller. This is evident in the 5G revolutions taking place in the telecommunications sector the world over and its relative minor cost. It is also worth noting that the major oil companies, both private and state-owned, were global but rooted in a particular nation-state: BP began as *British* Petroleum. Now, the allegiances of at least the tech giants outside China—the "big five" (Apple, Alphabet, Microsoft, Facebook, and Amazon)—are more in question despite their origins in the United States.

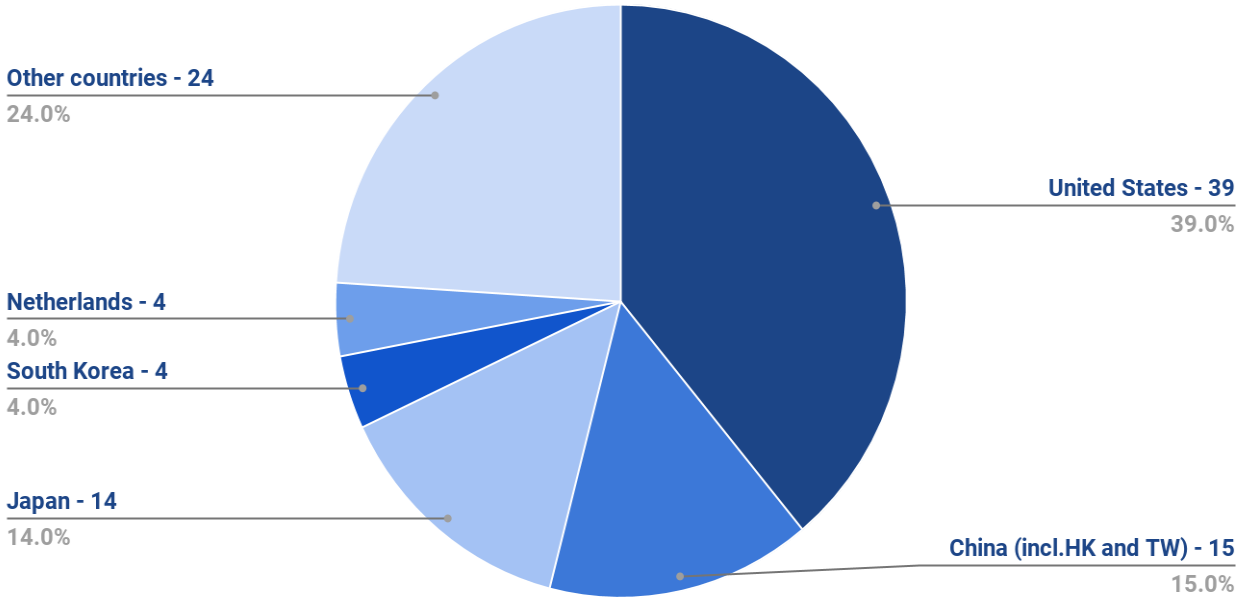
[4] Gregory F. Treverton and Pari Esfandiari, "Data Has Paralleled Oil in Becoming an Intensely Political National Security Issue," *The Hill*, September 14, 2019, https://thehill.com/opinion/national-security/461420-data-has-paralleled-oil-in-becoming-an-intensely-political-national.

The 10 Largest Tech Companies in the World[5]

Rank	Company	Country	Market Cap	Assets
1	Apple	United States	$2T	$320.4B
2	Microsoft	United States	$1.63T	$285.4B
2	Alphabet	United States	$1.03T	$273.4B
4	Samsung Electronics	South Korea	$278.7B	$304.9B
5	Intel	United States	$224.64B	$147.7B
6	Facebook	United States	$753.37B	$138.4B
7	Tencent Holdings	China	$509.7B	$137B
8	IBM	United States	$113.81B	$153.4B
9	Cisco Systems	United States	$168.7B	$90.4B
10	Oracle	United States	$184.12B	$96.7 B

[5] This table was compiled using data from Murphy et al., "Global 2000: The World's Largest Public Companies," *Forbes*, May 13, 2020, https://www.forbes.com/global2000/#5154c457335d. It is important to note that Amazon ranks above Intel but is categorized as a retailer rather than a tech company.

Where the Top 100 Digital Companies Are Located[6]



Data is information, and big data is often seen as simply lots of data; thus data, information, and big data overlap, and so do the issues involved in governing them. Those issues range from the seemingly prosaic (in what country will data centers be located?) to questions bearing on the nature of democracy itself (how will false news and hate speech be policed, and by whom?). In the process, how data is collected, stored, protected, accessed, used, and transferred over national borders is becoming caught up in geopolitics.

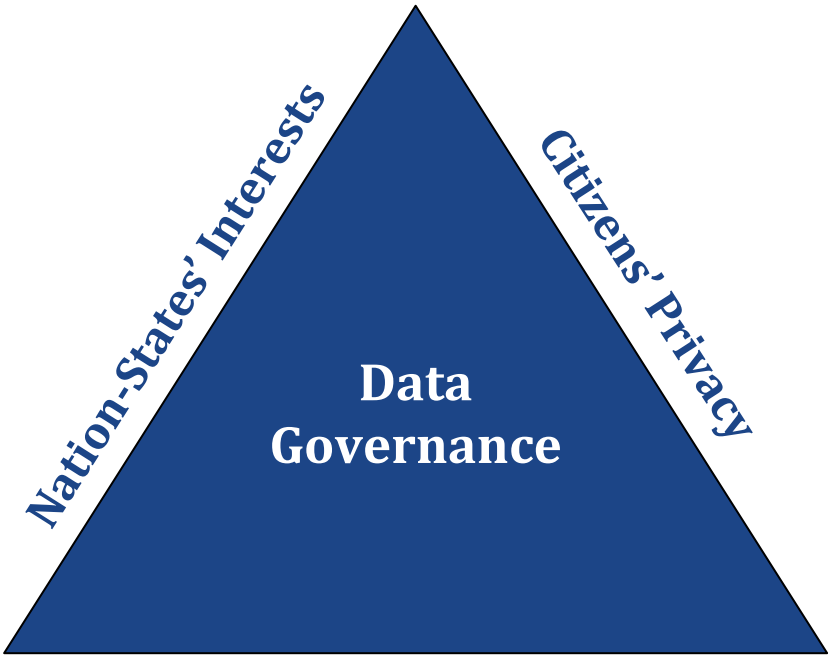
Governance has become a hackneyed word, but to the extent that data is governed, that governance is a byproduct of internet governance, or the lack thereof. The World Summit on the Information Society (WSIS) in 2005 defined governance for the internet as "the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet." This UN-sponsored summit also formed the Internet Governance Forum (IGF) for an open

[6] This chart was compiled using data from Forbes, "Top 100 Digital Companies," 2019, https://www.forbes.com/top-digital-companies/list/2/#tab:rank. It is important to note that Forbes uses the term "digital company" broadly to cover companies from a variety of fields, including telecommunications, entertainment streaming services, internet & catalog retail, electronics, software and programming, etc.

discussion on the future of internet governance. With no commitments yet, the Forum has accomplished nothing of operational significance thus far.[7]

Overall, internet governance is scattered, multi-stakeholder, bottom-up, and driven by loose coordination among various players.[8] Data governance, largely derivative of internet governance, is similar. It is best thought of as a triangle that incorporates citizens and their privacy, nation-states and their interests, and the private sector and its profits. Its current status and prospects might be thought of along several lines of activity, which are interrelated but, for the sake of clarity and with some danger of oversimplification, are discussed in the following sections: legislating privacy and data use, regulating to police content, using antitrust to dilute data monopolies, self-regulating by the tech giants, regulating digital trade, addressing intellectual property rights (IPR) infringement, assuring cybersecurity, and practicing cyber diplomacy.

The Triangle of Data Governance



[7] World Summit on the Information Society, "Tunis Agenda for the Information Society," Nov.18, 2005, http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.
[8] Jonathan Masters, "What Is Internet Governance?," *Council on Foreign Relations*, April 23, 2014, https://www.cfr.org/backgrounder/what-internet-governance.

The history of ICANN, the Internet Corporation for Assigned Names and Numbers)—which supervises the assignment of domain names, internet protocol addresses, and other key web particulars)—nicely illustrates the structure of internet governance: the corporation evolved out of the early U.S. ARPANET pioneers—indeed, one of those pioneers, Jon Postel, performed the ICANN functions on his own for a prolonged period—and was closely connected to the U.S. Department of Commerce before becoming fully independent of the government in 2016. Now it is a private nonprofit headquartered in California but is still often suspected of being too U.S.-centric in its approach.

Any discussion of data governance inevitability must address the different visions of the internet and the future we desire.[9] Concepts range from Silicon Valley's open internet and free flow of data with the faintly anarchist motto "data wants to be free" to Washington's market-based internet—if data is the new oil, then let's drill it.[10] This stands in contrast to the EU's bourgeois approach to internet governance, which seeks to maximize freedom for online users but under tight government regulation. Further abroad, Beijing champions an authoritarian vision as represented by the Great Firewall, a tightly-controlled collaboration in which the government closely monitors technology and telecommunications companies, who enforce the state's promulgated rules.[11] Moscow's mule model aims to disrupt the international order while taking steps to test the independence of its internet by routing all traffic through exchange points controlled by its national regulator, Roskomnadzor.[12] This, in effect, gives the Russian government the ability to temporarily cut itself and its citizens off from the global World Wide Web. India, in contrast, takes a more ideological standpoint, namely of ensuring it is not "colonized" again by international Western firms managing its citizens' data. The varying approaches outlined above, and the ideological differences between them, compound the looming threat of the "splinternet"—a stratified global internet.

Add to this the fundamental cultural differences between various countries that influence their policies and approaches. For example, privacy has different meanings in China, the United States, and

[9] Kieron O'Hara and Wendy Hall, "There are now four competing visions of the internet. How should they be governed?," World Economic Forum, March 12, 2019, https://www.weforum.org/agenda/2019/03/there-are-now-four-competing-visions-of-the-internet/.
[10] Martin Heller, "Data Wants to be Free," InfoWorld, May 1, 2007, https://www.infoworld.com/article/2640847/data-wants-to-be-free.html.
[11] "The Great Firewall of China," *Bloomberg News*, November 5, 2018, https://www.bloomberg.com/quicktake/great-firewall-of-china.
[12] Louise Matsakis, "What Happens If Russia Cuts Itself Off From the Internet," *Wired*, February 12, 2019, https://www.wired.com/story/russia-internet-disconnect-what-happens/.

Europe. Since the internet is a global network of networks, national internet policies have global ramifications.

Issues in governing the digital domain overlap, cut across policy areas, and even conflict. For example, efforts to safeguard privacy conflict with national security requirements. Digital trade touches on all other policy areas and conflicts with some. Laws, standards, and norms that are required to safeguard universal values or global and national interests, such as the environment, human rights, and privacy, could limit the scope of free digital trade. The Organization for Economic Cooperation and Development (OECD) sets out three policy goals in the digital economy: "(1) enabling the internet; (2) boosting or preserving competition within and outside the internet; and (3) protecting privacy and consumers."[13] It goes without saying that the three can conflict with one another.

Different Visions of the Internet[14]	
Silicon Valley's Open Internet	This is a decentralized and anarchist vision of the internet, in which data flows are completely unrestricted.
Washington DC's Commercial Internet	The internet and data are viewed as resources that can be used by private actors for innovation and value creation. For the most part, the market governs itself, but a little government regulation now and then can be a good thing.
Brussels' Bourgeois Internet	The European Union's internet seeks to maximize freedom of expression while ensuring good behavior, privacy protections, and transparency. The key to this model is regulation.
Beijing's Paternal Internet	The Internet is viewed as a tool that should serve the public good. Thus, censorship is necessary to restrict access to any content the government deems harmful or undesirable. This vision is best demonstrated by China's Great Firewall.
Moscow Mule Spoiler Model	This is not a vision, but rather a strategy. This model is characterized by the use of the Internet as a tool for spreading disinformation and malware, engaging in cyberwarfare and cyberespionage, and overall breeding chaos.

[13] Koske et al., "The Internet Economy."
[14] Catherine Tsalikis, Kieron O'Hara, and Wendy Hall, "The Four Visions Shaping the Way We Use the Internet," *Centre for International Governance Innovation*, June 13, 2019, https://www.cigionline.org/articles/four-visions-shaping-way-we-use-internet.

LEGISLATING PRIVACY AND DATA USE

The focal points of legislation are privacy (what will happen to personal information collected by websites), accuracy (how users will know when something posted is false), decency (how users will be protected from harmful and hateful language or images), and stewardship (where and by whom will personal information be stored). The root of the challenge is that tech giants stumbled on to business models that are both hugely profitable and hugely predatory, as they depend on collecting, using, and selling personal information about users.

"The root of the challenge is that tech giants stumbled on to business models that are both hugely profitable and hugely predatory, as they depend on collecting, using, and selling personal information about users."

The more information, the better—as this allows for more personalized services and customized marketing.

In a striking demonstration of how much global geometry has changed, neither of the two most noted pieces of legislation about data privacy so far has been enacted by a nation-state. Most important is the European Union's General Data Protection Regulation (GDPR)—enforceable since May 2018—which is built on previous EU data protection laws.[15] GDPR stipulates how data controllers and/or processors must collect and process data from EU citizens, regardless of where they're located, requiring platforms to comply with GDPR standards in order to operate within the EU. This framework is accompanied by the Privacy and Electronic Communications Directive 2002 (ePrivacy Directive), which mandates that EU users who visit sites, irrespective of their location, must be told what data the site collects from them via cookies and users must explicitly agree to this. The European Commission has been working

[15] Jake Frankenfield, "General Data Protection Regulation (GDPR)," Investopedia, November 11, 2020, https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp.

to strengthen this legislative framework through the development of the ePrivacy Regulation, which would update—and in many cases tighten—rules related to data collection and privacy, replacing the current e-Privacy Directive. For now, the GDPR remains the principal regulatory tool, as the ePrivacy Regulation's consultation and amendment processes drag along slowly.

The other major piece of legislation is the California Consumer Privacy Act, or CCPA, which came into force at the beginning of 2020. In contrast to the GDPR, which in effect requires consumers to opt *into* data collection, the CCPA allows consumers to opt out. [16] In that sense, it is less stringent than the GDPR. The GDPR permits people to prevent the collection of their data before it is collected. In contrast, the CCPA permits companies the ability to automatically collect data on users but allows users to request that these activities be stopped.

The CCPA gives users the right to ask a company to produce all the personal information it has gathered on them over the years, as well as all the categories of businesses it got that information from or sold it to. If a consumer asks, in terms of both GDPR and CCPA laws, companies must delete all the information they have on that consumer, and if they have shared personal data with another company, they must ensure that any subsequent company processing that data deletes it too.

The EU's intention to create a much stronger and more robust privacy framework has been apparent since the early days of the web. The EU has signaled that its understanding of the right of privacy is not only different from many other nations but is also a high priority. The GDPR was preceded by the 2002 ePrivacy Directive, the landmark 2014 decision by the European Court of Justice on the Right to be Forgotten, and the 2017 ePrivacy Regulation proposal, which continues to be developed. The GDPR shifts the dynamic of personal data use towards users by giving them ultimate control over the processing of their data.[17]

This transatlantic difference was illustrated by an experiment conducted just before the GDPR came into force.[18] Researchers in Britain and the United States asked for information about data being processed about them from local companies in order to compare their responses. Researchers in Britain got "200

[16] For a detailed chart comparing GDPR and CCPA, see Laura and Alan Friel, "CCPA and GDPR Comparison Chart," *Practical Law,* nd, www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.
[17] Konstantinos Komaitis, "GDPR: Going Beyond Borders," Internet Society, May 25, 2018, www.internetsociety.org/blog/2018/05/gdpr-going-beyond-borders/.
[18] Natasha Singer and Prashant S. Rao. "U.K. Vs. U.S.: How Much of Your Personal Data Can You Get?" *The New York Times*, May 20, 2018, www.nytimes.com/interactive/2018/05/20/technology/what-data-companies-have-on-you.html.

rows of data" containing details about their personal lives and "343 rows of data on the consumer marketing segments" assigned to them. In comparison, those in the United States were furnished with 1 row of data indicating a Forbes article they had once read and noted that "the company responded to data access requests under European law. So sending me any data at all has been an error—because consumers in the United States do not have a comprehensive right to obtain copies of the data held by American companies."[19] From Amazon, the British residents received "order history, credit card information, prime subscription data addresses, wish list items, and devices used to access amazon services," while the American resident received only order history.[20] The contrast in approaches is evident and stark.

The GDPR both sought to be and is being used as a template for other countries.[21] Indeed, 132 out of 194 countries have put in place some legislation to secure data and privacy. Brazil, Japan, and South Korea have followed Europe's lead, and, in general, the EU has set a higher standard for not only privacy but also the enforcement of antitrust laws, leading to tougher tax policies. In contrast, the United States, especially under the Trump administration, has taken a different path with talk but little action about regulating the tech industry. Instead, it has sought to protect the big tech companies from taxes in foreign countries and limit regulation while, at the same time, protecting them from Chinese competition.[22]

Because GDPR has become the standard, any nation interested in a trade agreement with the European Union (EU) must address data privacy as a precondition. This is perhaps best demonstrated in the latest ruling of Schrems II, a landmark case which, for a second time, has invalidated the US-EU's long-standing data protection agreement.[23] As Dean C. Garfield, president of the Information Technology Industry Council put it, "in the absence of another approach, it's easier for other markets to follow what Europe has done." In fact, Microsoft allows users to manage their data according to GDPR rules, even if they aren't EU citizens. Other companies, including Facebook, are adjusting their privacy practices and tools on a global scale but without giving all users the same right the

[19] Singer and Rao. "U.K. Vs. U.S.: Personal Data."
[20] Singer and Rao. "U.K. Vs. U.S.: Personal Data."
[21] Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *The New York Times*, May 24, 2018, www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.
[22] Emily Taylor and Stacie Hoffman, "EU–US Relations on Internet Governance." Chatham House, November 14, 2019, www.chathamhouse.org/publication/eu-us-relations-internet-governance.
[23] Joshua P. Meltzer, "The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security," *Brookings*, August 5, 2020, https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.

GDPR provides or, arguably, any GDPR-associated right (as illustrated in Schrems II).

The difficulties of legislating borderless activities have been underscored by the OECD's struggle to negotiate a global consensus on digital taxation. The United States dropped out of the discussions in June 2020, apparently fearing that the "big five" companies were being targeted. The result is likely to be further balkanization of this aspect of internet governance, with individual countries imposing levies, thus pitting themselves against the United States, which, in turn, uses carrots and sticks to get the taxes negated or diluted.

Since European countries have been in the lead in pushing digital taxation, trans-Atlantic relations will likely suffer as a result. For instance, in 2019, France levied a 3 percent tax on the revenue companies receive from providing goods and services to French residents over the internet, even if the companies had no significant presence in France. In response, the United States began an investigation into whether that discriminated against the big five and others. In early 2020, the two countries declared a pause, with France agreeing not to collect the taxes while the OECD discussions continued. However, when the United States left those negotiations, it proceeded to announce tariffs on selected French goods in retaliation for the taxes.

Data protection and privacy laws do not usually require stewardship in the form of retaining data, and in principle protecting data would argue for not retaining copies at all. However, stewardship laws place restrictions on data flows, limiting data transfer over national borders according to certain data security and safety standards. The concept of privacy and over-border data flow has given rise to three terms—"data residency," "data sovereignty," and "data localization"—that are often used interchangeably, leading to confusion.

Data residency is where a site chooses to locate its data warehouses, a decision based on reasons that range from evading or benefiting from laws, regulations, and tax regimes to convenience and subjective preference. Once the location is selected, data is subject to local data residency laws, also known as data sovereignty. These laws are usually designed to protect government interests and often cover data likely to be core to the business model. They allow data transfer over the border but demand that sites keep a local copy available to the local government for inspection; an example is India's draft Personal Data Protection Bill.[24]

[24] Government of India, "The Personal Data Protection Bill," 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

Data localization—mandating that data acquired within a nation's borders remain there—is the most restrictive of the three concepts, and its application is growing rapidly. The Founder and CEO of Calligo, Julian Box, describes the concept as one "almost always applied to the creation and storage of personal data, with exceptions including some countries' regulations over tax, accounting, and gambling."[25] Here, the law prevents data from crossing the border. Russia's Personal Data Law (OPD-Law) is a case in point: storing, updating, or using data on Russian citizens must be confined to data centers inside Russia. Skeptics of these residencies and, especially, localization laws believe the argument that these laws secure the cyber realm or protect individual privacy is a cover for what is really trade protectionism, an issue covered in more depth in the trade section of this paper. When data is confined to national silos, the potential of that data is limited, and the ultimate result could be a splintering of the web— "splinternet" in the jargon of the trade.

"When data is confined to national silos, the potential of that data is limited, and the ultimate result could be a splintering of the web—'splinternet' in the jargon of the trade."

[25] Julian Box, "Data Sovereignty vs Data Residency vs Data Localization," Insights For Professionals, March 12, 2019, https://www.insightsforprofessionals.com/en-us/it/storage/data-sovereignty-data-residency-data-localization.

Relevant Legislation: Privacy and Data Use			
Year	Legislation	Enacted into Law?	Summary
2002, amended in 2009	The EU's e-Privacy Directive (ePD)[26]	Yes.	This law requires each EU member state to pass their own national data and privacy laws. The directive touches upon the issues of cookies, data anonymization, consent to data collection, and unsolicited messages.
2016, effective since 2018	The EU's General Data Protection Regulation (GDPR)[27]	Yes.	The GDPR is a legal framework that requires all sites, regardless of where they are based, follow certain data collection guidelines if they wish to be accessible to EU citizens. The principal requirement is that platforms must notify users of data collection, and users must explicitly consent to sharing their information.
2017 - 2020[28]	The EU's e-Privacy Regulation Draft[29]	Legislation still in development.	The e-Privacy Regulation proposal would replace the ePD and supplement the GDPR by updating—and in many cases tightening—rules related to data collection. One notable change is that the regulation would apply stricter privacy requirements to internet-messaging services.[30]

[26] The European Parliament and the Council of the European Union, Directive 2002/58/EC (Directive on privacy and electronic communications), EUR-Lex, July 12, 2002, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.
[27] The European Parliament and the Council of the European Union, General Data Protection Regulation, *Official Journal of the European Union*, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[28] For the latest amendments to the e-Privacy Regulation, see Council of the European Union, *Regulation on Privacy and Electronic Communications*, February 21, 2020, https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/02/CONSIL_ST_5979_2020_INIT_EN_TXT.pdf.
[29] The European Parliament and the Council of the European Union, *Regulation on Privacy and Electronic Communications*, EUR-Lex, October 1, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.
[30] For more information on the proposed changes under the e-Privacy Regulation, see "The new EU Privacy Regulation: what you need to know, I-Scoop, last updated May 19, 2020, https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/.

Relevant Legislation: Privacy and Data Use			
Year	Legislation	Enacted into Law?	Summary
2018, effective since 2020	The California Consumer Privacy Act (CCPA)[31]	Yes.	The CCPA secures the following privacy rights for California consumers: the right to know about the personal information a business collects about them, the right to delete personal information collected from them, and the right to opt out of the sale of their personal information.[32]
2019	India's Personal Data Protection Draft Bill[33]	No, awaiting approval.	If this bill is enacted, consumers would need to give consent to data collection and would also have the opportunity to withdraw this consent at any time. Online platforms would need to design systems that allow the consumer to "access, correct, and erase their data."[34]
2006, amended in 2014	Russia's Personal Data Law (OPD-Law)[35]	Yes.	The law contains strict data collection provisions relating to consent, the right to be forgotten, and the right to review. The bill was amended in 2014 to include clear data localization provisions, requiring data be stored and processed in Russian databases.[36]

[31] California Legislative Counsel, *SB-1121 California Consumer Privacy Act of 2018*, California Legislative Information, September 24, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.
[32] For more information on the CCPA, see "California Consumer Privacy Act (CCPA)," State of California Department of Justice - Attorney General Xavier Becerra, https://oag.ca.gov/privacy/ccpa.
[33] Government of India, *The Personal Data Protection Bill,* 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
[34] Anirudh Burman and Suyash Rai, "What Is in India's Sweeping Personal Data Protection Bill?," March 9, 2020, Carnegie India, https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985.
[35] "Federal Law No. 152-FZ of July 27, 2006: On Personal Data," Passed by the State Duma on July 8, 2006, Approved by the Federation Council on July 14, 2006, http://wko.at/ooe/Branchen/Industrie/Zusendungen/FEDERAL_LAW.pdf.
[36] Matthias Bauer et al., "Data Localisation in Russia: A Self-imposed Sanction," Policy Brief, *European Centre for International Political Economy*, No. 6, 2015, https://ecipe.org/wp-content/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.

REGULATING TO POLICE CONTENT

The challenge of regulation—that internet technologies move fast while governmental processes are slow and deliberative, especially if the action sought involves several nations and thus requires a treaty or international agreement—also afflicts legislation.[37] As a result, there is always the inherent risk that by the time a regulation is enacted, it will be obsolete or, worse, counterproductive.

The challenge is illustrated by one old piece of legislation that has come under new scrutiny: Section 230 of the U.S. Communications Decency Act of 1996. Enacted in the early years of the web, its goal was to promote innovation, not to protect decency or privacy. As a result, the regulatory regime it established was permissive: providers were given broad immunity from lawsuits for words, images, and videos posted on websites.

It is increasingly the target of criticism across the political spectrum.[38] President

"The challenge of regulation—that internet technologies move fast while governmental processes are slow and deliberative, especially if the action sought involves several nations and thus requires a treaty or international agreement—also afflicts legislation."

Trump and the political right believe Twitter, Facebook, and their kin muzzle conservative views, and without the 230 protections, voices who felt they had been denied a platform could have sued. The other side of the political spectrum, including House Speaker Nancy Pelosi, maintains that Section 230 has permitted a slew of disinformation and harassment, and absent it, they argue, the sites would have to be much more careful in policing their

[37] Patrick, Stewart M., and Naomi Egel, "Governing the Internet: The Latest Addition to the Global Governance Monitor," *Council on Foreign Relations*, October 20, 2015, www.cfr.org/blog/governing-internet-latest-addition-global-governance-monitor.
[38] Bobby Allyn, "As Trump Targets Twitter's Legal Shield, Experts Have A Warning." *NPR*, May 30, 2020, https://www.npr.org/2020/05/30/865813960/as-trump-targets-twitters-legal-shield-experts-have-a-warning.

content. A 2019 bill introduced by Senator Josh Hawley (R-MO) proposed ending legal protections for tech companies that did not agree to an independent audit ensuring that there was no political bias to their monitoring of content. Sen. Hawley's May 2020 bill—The Limiting Section 230 Immunity to Good Samaritans Act—allows for civil liability of up to $5,000 against tech giants. These bills are among dozens of other proposed technology-related bills in Congress awaiting approval.

Comparing the experiences of other countries in regulating internet content is instructive. India has the second oldest legislation on the topic, passed in 2000, which, like the U.S. Communications Decency Act of 1996, gave sites safe harbor from liability but, unlike the U.S. act, did so only if the site met stipulated conditions.[39] Those conditions were extended in 2011 to include more types of content that should be taken down once a website was made aware of them by users. Another bill, proposed in 2018 but not yet enacted, would require platforms to be proactive in monitoring, taking down illegal content within twenty-four hours when flagged by a court order or government agency.

Likewise, in 2000, the EU issued its own e-commerce directive, which paralleled India's approach by providing a safe harbor from liability, provided the site was a "mere conduit" that removed the highlighted material once it was brought to their attention.[40] As in the United States, technological change has scrambled the debate with calls for revision of the directive. Twenty years later, the EU is finally updating this framework with its Digital Services Act, which would increase protections for users through "a modern system of cooperation for the supervision of platforms" and enact a broad range of rules for gatekeeper platforms to ensure digital market competition and innovation.[41] Yet, the EU's legislative process is slow and tedious, prompting member EU states to move ahead on their own. For example, Germany's 2017 Network Enforcement Act (NetzDG) and France's 2020 "Fighting hate on the Internet" bill clarifies the conditions under which tech platforms are fined for disseminating illegal or harmful content. When users identify such content, the platforms are given only a brief period—twenty-four hours in Germany and France—to take it down. The laws stop short of requiring constant monitoring, but they surely would lead to much more restrictive moderating by the sites themselves.

[39] For comparisons of internet regulation in several countries, see David Morar and Bruna Martins dos Santo, "Online content moderation lessons from outside the US", *Brookings*, June 17, 2020, https://www.brookings.edu/blog/techtank/2020/06/17/online-content-moderation-lessons-from-outside-the-u-s/.
[40] Morar and Martins dos Santo, "Online content moderation."
[41] European Commission, "The Digital Services Act Package," last updated June 22, 2020, https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

In 2019, the United Kingdom, soon to leave the EU, released a government white paper that goes well beyond the EU's provisions.[42] In addition to requiring, as the EU does, platforms to have some mechanism for taking down unlawful content, it calls for an undefined "duty of care." Presumably, this would include proactive and constant monitoring of web content, supervised by a new regulatory agency with the authority to create and enforce best practices, including by issuing fines and even imposing prison sentences.

Adapting to the new realities is not just a challenge for the United States; the law France passed required sites to take down hateful content flagged by users and to do so within twenty-four hours, but the French Constitutional Court ruled in mid-2020 that putting the onus only on the tech companies with heavy fines would encourage tech platforms to indiscriminately remove content without proper evaluation and consequently infringe on free speech.

"Comparing the experiences of other countries in regulating internet content is instructive."

[42] UK Department for Digital, Culture, Media & Sport, "Online Harms White Paper", February 12, 2020, https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

Relevant Legislation: Content Regulation			
Year	Legislation	Enacted into Law?	Summary
1996	Section 230 of the U.S. Communications Decency Act[43]	Yes.	This regulatory framework focuses on protecting freedom of speech and innovation online. Section 230 provides broad protections for online providers that host or republish content, allowing them to escape legal responsibility for hate speech, misinformation, disinformation, etc.
2019 - 2020	The U.S' The Limiting Section 230 Immunity to Good Samaritans Act[44]	No, awaiting approval.	If enacted into law, this bill would require tech platforms to "update their terms of service to operate under a clear good faith standard and pay a $5,000 fine if they violate those terms."[45]
2000, amended in 2008 and 2011	India's Information Technology Act[46]	Yes.	This act includes a broad range of cyber-related rules that legally define cybercrime offenses, provide legal recognition to e-commerce transactions, and provide safe harbor from liability for providers that publish third-party content. In 2008, the act was amended to allow for greater regulation, including penalties for offensive or harmful content.
2018	India's Information Technology (Amendment) Draft[47]	No, awaiting approval.	This bill would significantly increase content moderation, requiring platforms to employ artificial intelligence (AI) tools to identify and remove unlawful content. It would also limit the takedown window for unlawful content to 24 hours, if prompted by a court order or government notification.

[43] U.S. Congress, U.S. Code § 230 - Protection for private blocking and screening of offensive material, Cornell Law School Legal Information Institute, https://www.law.cornell.edu/uscode/text/47/230.
[44] U.S. Congress, S. 3983, June 17, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3983/text.
[45] "Rubio, Hawley Announce Bill Empowering Americans to Hold Big Tech Companies Accountable for Acting in Bad Faith," Marco Rubio - US Senator for Florida, June 17, 2020, https://www.rubio.senate.gov/public/index.cfm/press-releases?ContentRecord_id=47276D77-62D6-4E04-9FA2-1CD761179B90.
[46] Government of India, The Information Technology Act, 2000, https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf.
[47] Government of India, The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018, https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

Relevant Legislation: Content Regulation			
Year	Legislation	Enacted into Law?	Summary
2002	The EU's e-Commerce Directive (eCD)[48]	Yes.	Like India's IT Act, the EU's e-Commerce Directive provides online providers with exemptions from liability for third-party content published on their sites but requires that providers remove unlawful content once notified.
2020	The EU's Digital Services Act[49]	Legislation not yet introduced.	The Digital Services Act would update the EU's e-Commerce Directive to allow for greater content regulation, as well as greater competition and innovation in the digital market.
2020	France's "Fighting hate on the Internet" bill[50]	Yes, but later struck down by the French Constitutional Court.	The law would have obligated platforms to take down hateful or abusive content within 24 hours of it being flagged by users.
2017	Germany's Network Enforcement Act (NetzDG)[51]	Yes.	The law allows the government to fine social media platforms up to €50 million if they fail to remove "fake news" or harmful content within 24 hours of it being reported.
2020	The UK's Online Harms White Paper [52]	Legislation not yet introduced.	This white paper proposes a regulatory framework to remove harmful or illegal content as well as prevent terrorists from using the internet to spread propaganda and radicalize vulnerable individuals.

[48] European Parliament, Council of the European Union, Directive 2000/31/EC of the European Parliament and of the Council, June 8, 2000, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031.
[49] European Commission, "The Digital Services Act package."
[50] France - Conseil Constitutionnel, "Décision n° 2020-801 DC du 18 juin 2020", June 18, 2018, https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.
[51] Bundestag (German Federal Parliament), "Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG)," German Law Archive, September 1, 2017, https://germanlawarchive.iuscomp.org/?p=1245.
[52] UK, "Online Harms."

USING ANTITRUST LAW TO DILUTE DATA MONOPOLIES

Today's antitrust proposals are, not surprisingly, aimed at reducing concentrations of data—for instance, Facebook spinning off WhatsApp or Instagram, or Amazon spinning off its cloud division, Amazon Web Services. However, antitrust law is intended to protect competition, not competitors, so sheer size alone is hardly decisive: Starbucks is enormous, but that alone doesn't prevent a lone entrepreneur from doing just what Starbucks did decades ago in a Seattle corner coffee shop. Moreover, proving that consumers are harmed by huge tech companies is elusive when the services they offer cost little or nothing—at least in terms of money as opposed to surrendering personal data. [53]

The most celebrated antitrust case in the tech field, which took place more than two decades ago, was only indirectly about data. The issue was whether Microsoft had created a monopoly in operating systems and browsers for Intel-chip-based computers. The company had begun to bundle its operating system—Windows, with its browser, Internet Explorer—in effect eliminating the need for users to buy other browsers, and thus pricing them out of the market. The bundling was thought to have been the key to Microsoft's victory in the browser wars of the 1990s. The judgment went against Microsoft in late 1999, and the company was forced to split into two companies, one responsible for the operating system and the other for software, such as Microsoft Office and Internet Explorer.[54]

For most observers, the antitrust stakes are higher now even though, in the United States, there has been more talk and investigation than action. The U.S. Justice Department opened a probe into Google in late 2019, asking the company to provide documents relating to previous investigations by the Federal Trade Commission (FTC). Additionally, the Trump administration has considered taking Google to court over abusing its

[53] Kiran Stacey, Kadhim Shubber, and Hannah Murphy, "Which antitrust investigations should Big Tech worry about?," *Financial Times*, October 28, 2019, https://www.ft.com/content/abcc5070-f68f-11e9-a79c-bc9acae3b654.
[54] Antonio G. Martínez, "What Microsoft's Antitrust Case Teaches Us About Silicon Valley" *Wired*, February 11, 2018, www.wired.com/story/what-microsofts-antitrust-case-teaches-us-about-silicon-valley/.

power in the market for advertising technology and search products. Earlier, in 2012, the Federal Trade Commission had decided not to sue Google. This time around, the push to action is tinged by the familiar complaint from the political right that social media platforms suppress conservative views.

The FTC has also been looking into whether Facebook abused its market position by cutting off smaller rivals' access to data while maintaining exclusive partnerships with other potential competitors. The question at issue is whether customers would be able to choose a social media platform that extracted less data if there were more competition in the sector. However, FTC actions seldom break up companies. Instead, investigators usually opt for a less dramatic remedy. For instance, one possibility being discussed would compel tech giants to share their data in some way with competitors or new entrants. In an effort to ensure fair market practices, congressional committees have asked for documents from Google, Amazon, Facebook, and Apple, and at the state levels, at least two separate investigations are underway—one probing Google and involving all fifty state attorneys general, and another probing Facebook involving forty-seven.

Abroad, in 2020, Germany's highest court ruled that Facebook broke concentration (antitrust) laws when it combined data from its different platforms, especially WhatsApp and Instagram, as well as other sites and apps. The ruling, which will be appealed, was a direct challenge to Facebook's business model, for it required that the company let users block the company from combining Facebook data with that of other sources.

SELF-REGULATION BY THE TECH GIANTS

Self-regulation by the tech giants themselves is a cat-and-mouse game, with the companies acting on their own lest they are forced by regulators to take action they find undesirable. According to the Internet Governance Forum, "Public and private regulation often overlap: the term 'regulated self-regulation' refers to an arrangement in which companies regulate themselves, while the state oversees to ensure that the system is functioning as required."[55]

A major advancement in self-regulation occurred in 2019 when Google announced that it would allow users to automatically delete data on their web searches, location history, and requests made to the company's virtual assistant. In mid-2020, it announced that, for new accounts, it would automatically delete location history, records of web and app activities, and voice recordings after eighteen months. For skeptics of self-regulation, the changes are mostly window dressing. Facebook's newly introduced Internal Oversight Board is cited as an example.[56] It is meant to deal with the hardest cases but will hear only individual appeals about specific content that has been taken down—and will be able to hear only a fraction of these appeals. Content that has been left up will not be reviewed, nor will the board have authority over Facebook's advertising or the collection of data that makes Facebook ads so valuable. Finally, and most importantly, Facebook's algorithms that determine what content is seen most will remain intact.

The financial services industry offers one hybrid model for regulation: the Financial Industry Regulatory Authority (FINRA), which is licensed by Congress but is a private non-profit organization. Its mission is, in the language of its website, "making sure the broker-dealer industry operates fairly and honestly. We oversee more than 634,000 brokers across the country—and analyze billions of daily market events. We use innovative artificial

[55] Internet Governance Forum, "These Organisations Are Shaping the Internet: The Most Important Internet Governance Actors," May 23, 2019, www.igf2019.berlin/IGF/Redaktion/EN/Artikel/internet-governance-actors.html.
[56] Siva Vaidhyanathan, "Facebook and the Folly of Self-Regulation," *Wired*, May 9, 2020, www.wired.com/story/facebook-and-the-folly-of-self-regulation/.

intelligence (AI) and machine learning (ML) technologies to keep a close eye on the market and provide essential support to investors, regulators, policymakers, and other stakeholders."[57] Tech companies themselves could create something similar with guarantees of independence in their judgments and, ideally, with a license from Congress.

Recent debates about self-regulation have focused more on content than user data. There surely is a political overtone to much of the disinformation during the COVID-19 pandemic, but at least the task for tech giants has been relatively straightforward: warn users of wrong or misleading statements, especially dangerous ones, and take those down while guiding users to helpful information. Twitter, for example, acted early in the pandemic to try to assure that people looking for information on the virus were taken to reliable sources, like the World Health Organization or national health agencies, not conspiracy sites or outlets that had been identified as spreading "fake news."[58] As the crisis developed, Twitter's algorithms detected and flagged harmful falsehoods for removal—for instance, sites that were denying or advising against following official advice or promoting unproven "alternative" treatments.

Our partners at the Atlantic Council have started work on data trusts to guide and pace the recovery of economies from the COVID-19 pandemic.[59] Information in the trust would include where facilities had been cleaned, where it was safe to return to work, the state of safety procedures at particular facilities, whether public transportation is running and how clean it is, among other associated queries. The keys are transparency and trust. For, say, a metropolitan area, open protocols would specify what data would be collected and how it would be used, both routinely as economic recovery proceeds apace and in special contingencies that necessitate private-public cooperation—like the resurgence of the novel coronavirus in the summer of 2020. The project would include a continuous audit of how well the data is performing in the recovery, as well as how well those using it are adhering to the agreed-upon ethical standards and arrangements for governance.

The 2020 elections demonstrated the importance and urgency of transparency with regard to data governance over political content. Political advertising and the handling of content from politicians, in

[57] FINRA, https://www.finra.org/about.
[58] Bernard Marr, "Coronavirus Fake News: How Facebook, Twitter, and Instagram Are Tackling the Problem," *Forbes,* March 27, 2020, https://www.forbes.com/sites/bernardmarr/2020/03/27/finding-the-truth-about-covid-19-how-facebook-twitter-and-instagram-are-tackling-fake-news.
[59] David Bray, "We Can Increase Public Participation in Data and Avoid Surveillance States: Here Is How," *Atlantic Council*, July 1, 2020, https://www.atlanticcouncil.org/blogs/geotech-cues/we-can-increase-public-participation-in-data-and-avoid-surveillance-states-here-is-how/.

particular President Trump, have been controversial issues. Facebook has maintained the view that content that is false or divisive but from an important political figure should not be policed because it is in the public interest to view it. In contrast, Twitter earned Trump's scorn by beginning to fact check and add warnings to his tweets. In June 2020, Facebook, under pressure over hateful speech from its largest advertisers, including Coca-Cola and Starbucks, said it would attach labels to any posts that discuss voting, directing users to accurate voting information in an effort to prevent disenfranchisement. It also expanded the category of hateful language to be prohibited. Posts that violate those rules but are from senior politicians, like President Trump, will receive a label indicating the post was deemed noteworthy enough to remain.

Challenges to Industry Self-Regulation[60]

- ***Strength of instruments***. Instruments might have to be watered down to achieve industry support and therefore might not be sufficiently strong.
- ***Compliance and oversight.*** In the absence of effective enforcement and monitoring, participants might have little incentive to adhere fully to the scheme.
- ***Risk of regulatory capture.*** This could occur when a self-regulatory body is overly "close" to the businesses that it oversees.
- ***Free-riders.*** Businesses that do not participate in an ISR are not bound by its provisions and avoid the cost of compliance; they may benefit significantly from the avoidance of formal government regulation that might otherwise apply.
- ***Market coverage.*** Low participation rates by businesses in an ISR could render it ineffective.
- ***Favoritism.*** If a small number of actors dominate the governance of a scheme, it might result in the scheme favoring those actors.
- ***Distortions in competition.*** Self-regulation can create barriers to entry or otherwise distort competition through, for example, licensing or accreditation bodies that discriminate against certain businesses.
- ***Accountability***. Some self-regulatory schemes might lack mechanisms for review and evaluation, and resources may not be available if the schemes do not fulfil their objectives.
- ***Costs.*** The cost of establishing and operating an ISR might be high and passed on to consumers.

Source: OECD, 2015

[60] These ISR challenges were outlined by OECD, "Industry Self Regulation: Role and Use in Supporting Consumer Interests", *OECD Digital Economy Papers*, No. 247, OECD Publishing, Paris, March 1, 2015, p. 6-7, http://dx.doi.org/10.1787/5js4k1fjqkwh-en.

REGULATING DIGITAL TRADE

Given that data is now a precious commodity as well as a source of power, data flows across borders have become important for global trade and are subject to the existing global trade system. That system was created after World War II to promote global prosperity by reaching the General Agreement on Tariffs and Trade (GATT) in 1947. GATT reflects the conviction that free trade will result in global good, a belief as old as Adam Smith's *The Wealth of Nations* (1776). The goal is to lower tariffs, quotas, and other barriers to global trade through multilateral agreements. GATT rapidly evolved into the premier multilateral trade arrangement and succeeded in lowering average tariffs among industrial countries from around 40 percent at the start to about 5 percent today.

In 1995, the GATT was replaced by the World Trade Organization (WTO), which currently has 164 members and twenty-four observer governments. It is where members negotiate reductions in trade barriers and mediate disputes among themselves over trade matters. The WTO governs four global trade agreements: the GATT[61], the General Agreement on Trade in Services (GATS) [62], and the agreements on trade-related intellectual property rights[63] and trade-related investment[64] (TRIPS and TRIMS).

GATT signatories must extend most-favored-nation (MFN) status to all WTO members. Slightly odd given the language, MFN status means that no member's goods should be subject to tariffs in foreign markets higher than the lowest applied to any foreign country competing in that market. Most-favored-nation has been replaced in U.S. legislation with "normal trade relations (NTR)," which has the same meaning. However, GATT permits two exceptions from NTR: free trade areas, which let members eliminate tariffs on trade with each other but give them the right to set tariffs on non-members; and customs zones, which also eliminate tariffs among members but sustain a common tariff on countries that are not part of the union.

Over the last few decades, not surprisingly, digital trade has become a major part of

[61] WTO, "GATT and the Goods Council," https://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm.
[62] WTO, *General Agreement On Trade in Services*, 1995, https://www.wto.org/english/docs_e/legal_e/26-gats.pdf.
[63] WTO, "Overview: the TRIPS Agreement," https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.
[64] WTO, "Agreement on Trade Related Investment Measures," https://www.wto.org/english/tratop_e/invest_e/invest_info_e.htm.

trade flows. A joint Huawei-Oxford Economics report found that "the digital economy is worth $11.5 trillion globally, equivalent to 15.5 percent of global GDP and has grown two and a half times faster than global GDP over the past 15 years."[65]

What constitutes digital trade varies depending on which country one examines. The U.S. International Trade Commission (USITC) defines it as "the delivery of products and services over the internet by firms in any industry sector and of associated products such as smartphones and internet-connected sensors. While it includes the provision of e-commerce platforms and related services, it excludes the value of sales of physical goods ordered online and physical goods that have a digital counterpart, such as books, movies, music, and software sold on CDs or DVDs."[66]

The absence of a globally agreed-on definition of digital trade means there is also no set of international law to govern it, and that key issues are treated differently in different trade agreements. The WTO General Agreement on Trade in Services (GATS), for instance, predates the explosion of the global data flows across the internet, but since it does not distinguish how services are delivered, it includes digital services. Most other agreements, however, cover physical goods and intellectual property and make no provision for digital goods. However, since 1998, WTO countries have agreed on a series of moratoriums on imposing customs duties on electronically-transmitted services and goods, like e-books and music downloads.

"The absence of a globally agreed-on definition of digital trade means there is also no set of international law to govern it, and that key issues are treated differently in different trade agreements."

For its part, the WTO Information Technology Agreement (ITA) seeks to reduce tariffs not on goods traded on the internet but on the goods that enable it, aiming to lower the cost of IT products all along the value chain. The original agreement was reached in 1996 and was expanded to encompass further tariff cuts beginning in 2016. Its fifty-four

[65] Huawei Technologies Co. and Oxford Economics, Digital Spillover: Measuring the true impact of the digital economy, https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf.
[66] US International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, David Coffin et al., August 2017, 33, https://www.usitc.gov/publications/332/pub4716.pdf.

member countries are responsible for more than 90 percent of global trade related to the goods covered. Some member countries, like Vietnam and India, chose not to join the expanded agreement; however, as with the original ITA, all WTO members will receive the benefits of the expanded agreement on an MFN basis. ITA members will continue to review the agreement to see if emerging technology requires covering additional products. Tariff-cutting through the ITA has expanded trade in the technology that is the basis of digital commerce, yet the agreement neither tackles nor aspires to tackle the non-tariff barriers (NTBs) that limit trade.

There are increasing concerns about the WTO's ability to keep up with the mushrooming digital economy and digital trade. GATS is an example, for while it does cover electronic trade in services, it does so on what is called a "positive list" basis, wherein each member must opt in to a specific service sector for it to be covered. As a result, coverage across members varies, all the more so because many of today's digital goods and services had not yet been created when the agreements were reached. To address this shortcoming, the WTO's Committee on Specific Commitments is examining how both new digital services and new regulations, like data localization, could be addressed by GATS.[67]

The historical focus of trade policy has been visible barriers like tariffs and quotas. Efforts to reduce non-tariff barriers (NTBs) aim at broader governance issues, ranging from transparency and investor protections to restrictions on investment, foreign ownership, or people's movements. In the digital domain, privacy protection or national security arguments—often motivated by a different vision of the internet, as in the case of the EU, or as part of a grand geopolitical strategy in the case of China, or even a mixture of the two— are used to justify data localization measures.

As an example, from one perspective, China's insistence on internet sovereignty and full government control could be a legitimate effort to control harmful or hateful information. Yet, from another perspective, it is an NTB that limits foreign access to China's digital market, thus advancing Chinese corporations and limiting China's reliance on foreign technology.

By the same token, data localization measures also could be seen as NTBs, for they explicitly aim to limit flows across borders by requiring companies to store and process data within national borders.[68] They reduce efficiency by increasing costs and decreasing scale, effects that spill over into the entire global supply chain.

[67] World Trade Organization, "WTO members hold the latest 'cluster' of services meetings," March 21, 2019, https://www.wto.org/english/news_e/news19_e/serv_21mar19_e.htm.
[68] U.S. International Trade Commission, Digital Trade in the U.S. and Global Economies, Part 1, Publication No: 4415, Investigation No: 332-531, July 2013, p. 16, https://www.usitc.gov/publications/332/pub4415.pdf.

The data "silos" created by the localization requirement become valuable targets for a cyberattack, and localization discourages small and medium-sized companies from moving to cloud computing, which denies revenues to the largest global providers—all American companies: Amazon, Microsoft, Google, and IBM.

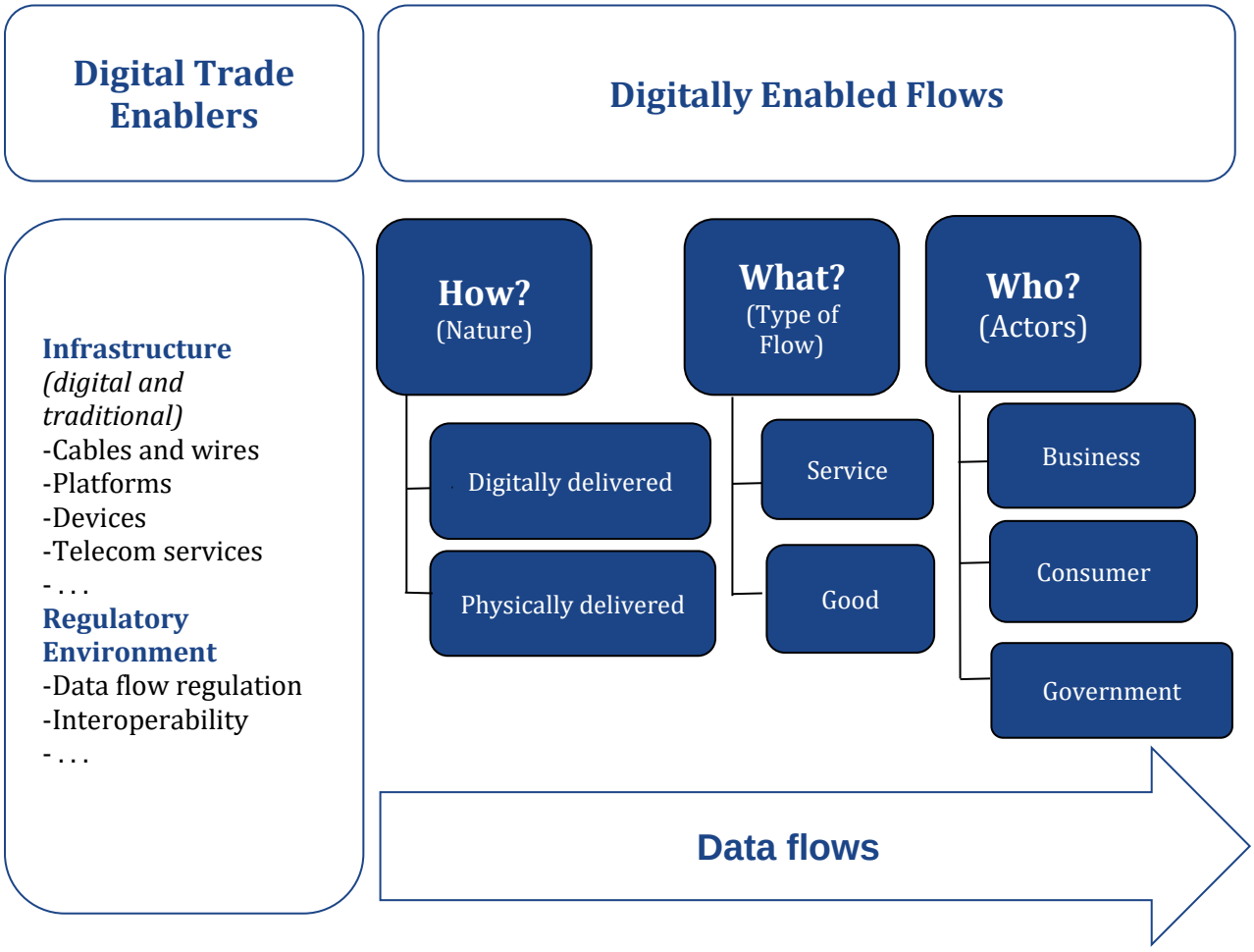
Other localization provisions that act like NTBs are familiar from trade in goods—for instance, the obligation to use local content and vendors for both hardware and/or software in order to operate or qualify for government contracts, or to partner with and transfer technology to local companies.

A Congressional Research Service (CRS) report, Digital Trade and U.S. Trade Policy, lists the following as barriers affecting digital trade: high tariffs, localization requirements, cross border data flow limitations, IPR infringement, discriminatory, unique standards or burdensome testing, filtering or blocking, restrictions on electronic payment systems or the use of encryption, cybertheft of U.S. trade secrets, and forced technology transfer.[69] Finally, net neutrality is an attempt, among other things, to purportedly prevent NTBs by protecting content providers from discrimination that internet service providers might otherwise impose.

"There are increasing concerns about the WTO's ability to keep up with the mushrooming digital economy and digital trade."

[69] Congressional Research Service, Digital Trade and U.S. Trade Policy, May 21, 2019, https://fas.org/sgp/crs/misc/R44565.pdf.

A Typology for Digital Trade[70]



Source: Lopez-Gonzales and Jouanjean, OECD, 2017.

[70] Javier Lopez-Gonzales and Marie-Agnes Jouanjean, "Digital trade: developing a framework for analysis," OECD Trade Policy Papers, No. 205, OECD Publishing, Paris, July 27, 2017, p.18, http://dx.doi.org/10.1787/524c8c83-en.

Digital Trade Barriers

Source: Digital Trade and U.S. Trade Policy May 21, 2019 - Congressional Research Service

Barriers to Internet Services

- Discriminatory treatment of digital goods and services
- Duties on digital goods or services
- Foreign investment restrictions
- Intermediary liability without safe harbor or fair-use provisions that could make internet platforms responsible for content posted by users
- Low de minimis threshold for customs duties on imported goods, including e-commerce purchases
- "Snippet tax" on search engines that quote text snippets as part of search results
- Taxes on over-the-top (OTT) services such as media, messaging, or voice-over-internet-protocol (VOIP)
- Web filtering and blocking of content

Localization Barriers

- Data localization requirements prohibiting cross-border data flows and requiring the use of local servers for data storage or processing
- Limited or no access to foreign government procurement markets
- Requirement for use of local technology
- Comprehensive privacy regulations that may discriminate against foreign providers

Technology Barriers

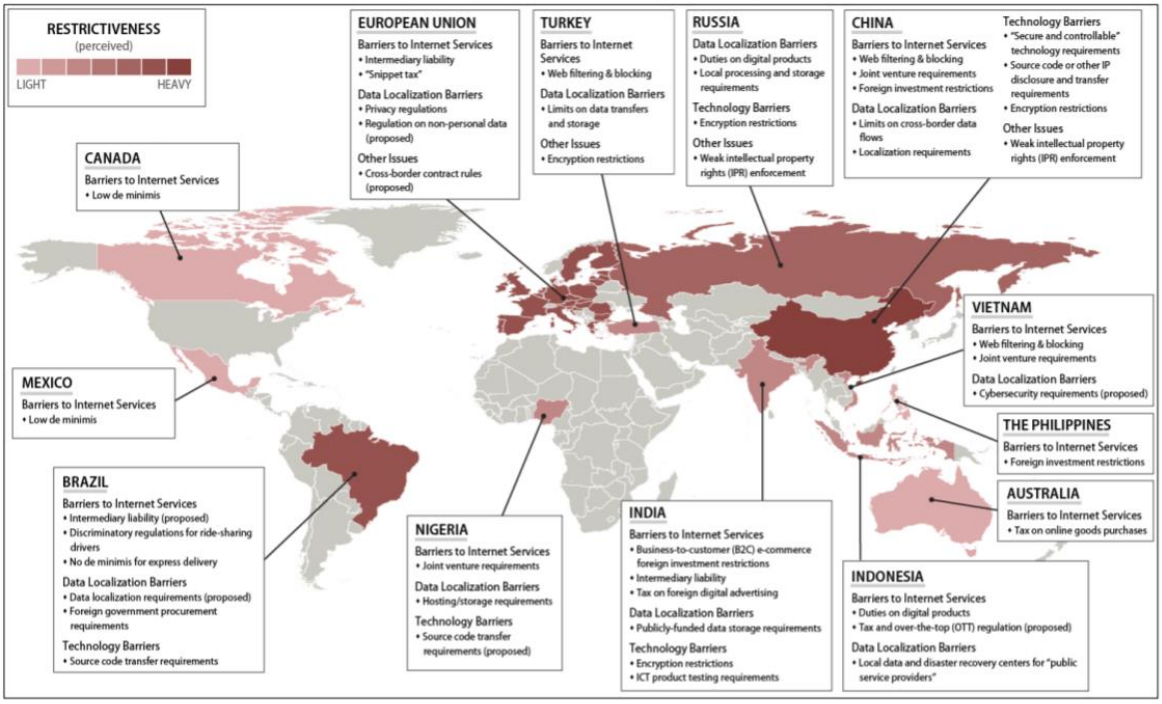
- Restrictions or prohibitions on use of encryption
- Source code, technology, or other intellectual property rights (IPR) forced transfer requirements
- Local testing and certification for imported information technology (IT) equipment may add costs or delays for imported goods

Other Barriers

- Cybersecurity threats or local requirements
- Weak IPR enforcement

Map of Perceived Digital Trade Barriers

Figure A-1. Levels of Perceived Digital Trade Barriers in Selected Countries
(according to the U.S. Trade Representative)



Source: CRS based on U.S. Trade Representative, *2018 National Trade Estimate Report on Foreign Trade Barriers.*
Note: This map is illustrative of digital trade barriers and not meant to be an exhaustive list.

In December 2017, over seventy WTO members reached an agreement to, as described in a WTO press release, "initiate exploratory work together toward future WTO negotiations on trade-related aspects of electronic commerce."[71] In January 2019, the statement was adopted by WTO's seventy-six partners, including both advanced economies, such as the United States, the EU, and Australia, and emerging economies, such as China and Brazil. India did not join because, as described by the CRS Report Digital Trade and U.S. Trade Policy, it preferred "to maintain its flexibility to favor domestic firms, limit foreign market access, and raise revenue in the future through potential customs duties."[72] The negotiating parties, despite their differences in the scope of the negotiations, have agreed to continue.

In recent years, multilateral agreements have come under attack by anti-globalists, who see them as serving the interests of

[71] WTO, "Joint Statement on Electronic Commerce," December 13, 2017, https://ustr.gov/sites/default/files/files/Press/Releases/Joint%20Statement%20on%20Electronic%20Commerce.pdf.
[72] Congressional Research Service, Digital Trade and U.S. Trade Policy, 34.

multinational corporations rather than people.[73] They argue that cost-cutting multinational corporations roam the globe in search of cheap labor and pliable regulations. This opposition has led to pressure to include various standards in trade agreements lest unrestricted trade should create a "race to the bottom" in labor, environmental, and other standards. The risk is that standards will become a pretext for protectionism by rich countries. Under these circumstances, it is no wonder that WTO negotiations have been stalemated: not only are the arguments complex, and the application of traditional trade policies to the digital economy unclear, but major players— the United States, the EU, and China—differ sharply in their approaches.

As a result, bilateral and regional trade agreements have become popular. One such agreement joins the United States and the EU, whose cross-border data flows are the largest in the world. The two also account for a big chunk of each other's e-commerce trade and almost half of each other's service exports that are delivered digitally.[74] Yet, different conceptions of data, trade, and privacy have driven a wedge between the two entities, forcing them to enter negotiations in 2013 over a vast array of digital and IPR trade topics that have yet to conclude.[75]

"... it is no wonder that WTO negotiations have been stalemated: not only are the arguments complex, and the application of traditional trade policies to the digital economy unclear, but major players— the United States, the EU, and China—differ sharply in their approaches."

The EU-U.S. Privacy Shield created a framework that companies could employ to protect personal data being transferred between the EU and the United States.[76] Companies could voluntarily certify that they had complied with, for instance, data processing requirements. The agreement also obliged the United States government to oversee and administer U.S. firms' compliance while establishing an ombudsman position and surveillance safeguards.

[73] Douglas A. Irwin, "International Trade Agreements," The Library of Economics and Liberty, https://www.econlib.org/library/Enc/InternationalTradeAgreements.html.
[74] Suominen, Kati, "Where the Money Is: The Transatlantic Digital Market," CSIS, October 12, 2017, https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/where-money-transatlantic-digital-market.
[75] European American Chamber of Commerce, "U.S. Objectives, U.S. Benefits In the Transatlantic Trade and investment Partnership: A Detailed View," March 11, 2014, https://eaccny.com/news/u-s-objectives-u-s-benefits-in-the-transatlantic-trade-and-investment-partnership-a-detailed-view/.
[76] Privacy Shield Framework, "Privacy Shield Overview," https://www.privacyshield.gov/Program-Overview.

However, in July 2020, the EU Court of Justice declared that the European Commission's decision that the shield provided adequate protection was "invalid." Thus, the shield no longer provides a way for firms to move data between the United States and the EU while staying in line with EU data protection requirements. The Privacy Shield Program Overview finding also noted that "this decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework."[77]

As noted earlier, the EU's General Data Protection Regulation (GDPR) is about data privacy, but also has trade ramifications—often referred to as the "Brussels effect": requiring the world to comply with its unilateral restrictions and, in turn, warranting data localization within the EU. In response to this, some large companies such as Amazon have taken steps to implement its requirements, but some businesses have simply chosen to forego the EU market instead.[78]

The Digital Single Market (DSM) is another attempt by the EU to create harmony across the region, part of continuing efforts to unify the EU market in order to promote trade and spur economic growth. It includes a mandate to allow non-personal information to freely cross borders, with only limited exceptions.[79] This mandate does not apply beyond the EU border.

Likewise, the United States has been actively establishing new digital trade rules in both its bilateral and plurilateral trade negotiations. In 2003 its Federal Trade Agreement (FTA) with Singapore included a chapter on e-commerce that has progressively evolved.[80] The US-South Korea FTA (KORUS) contains provisions on digital trade and explicitly addresses cross-border information flows.[81] The United States-Mexico-Canada Agreement (USMCA), which revised the trilateral North American Free Trade Agreement (NAFTA), established new rules in an effort to lower trade barriers, counter discriminatory actions, and put in place responsibilities on many elements of digital trade.[82]

[77] Privacy Shield Framework, "Overview."
[78] For a list of digital platforms that chose to block EU residents rather than comply with GDPR, see "Websites not Available in the European Union after GDPR," VerifiedJoseph, last updated April 26, 2019, https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr-2.
[79] European Commission, "Shaping the Digital Single Market," https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.
[80] Office of the United States Trade Representative, United States - Singapore Free Trade Agreement, May 2003, https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file708_4036.pdf.
[81] Congressional Research Service, The U.S.-South Korea Free Trade Agreement (KORUS FTA): Provisions and Implementation, Brock R, Williams et al., September 16, 2014, https://fas.org/sgp/crs/row/RL34330.pdf.
[82] Office of the United States Trade Representative, "United States-Mexico-Canada Agreement," https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement.

These bilateral and regional agreements remain controversial. Their proponents, like C. Fred Bergsten at the Peterson Institute for International Economics, call them "competitive liberalization," which challenges countries to keep up with other countries in reducing trade barriers.[83] In contrast, critics worry that the agreements will have the unintended effect of displacing trade from low-cost countries that are not adherents to the agreement to high-cost countries that are. This, according to them, undermines the multilateral WTO approach, which is preferable because it is global and non-discriminatory. They fear that, in the long run, bilateralism will fragment the world trade system into competing, discriminatory regional blocs, further complicating the flow of goods (and data) between countries. Moreover, some issues simply cannot be addressed effectively at the bilateral or regional level.

"… the United States has been actively establishing new digital trade rules in both its bilateral and plurilateral trade negotiations."

[83] C. Fred Bergsten, "Competitive Liberalization and Global Free Trade: A Vision for the Early 21st Century," Peterson Institute for International Economics, Working Paper 96-15, January 1996, https://www.piie.com/publications/working-papers/competitive-liberalization-and-global-free-trade-vision-early-21st.

Relevant Treaties and Legislation: Digital Trade		
Year	Treaty/Legislation	Summary
1947	General Agreement on Tariffs and Trade (GATT)[84]	The GATT was created to promote international trade through multilateral cooperation and reductions in tariffs and other trade barriers. Though the GATT predates the internet, it may still be applied to digitally-enabled and internet-era goods. For example, the GATT has "provided strong support for tariff reduction and elimination on ICT hardware."[85]
1995	General Agreement on Trade in Services (GATS)[86]	The GATS was created to reduce international trade barriers in the service sector. The GATS Annex on Telecommunications requires that governments allow for the transfer of data across borders, using telecommunications networks and services. This provision has been interpreted broadly to allow for greater applications in today's complex digital economy. For example, "if a government blocked data only for foreign or foreign-owned service suppliers benefiting from a GATS national treatment commitment, the discrimination would violate GATS Article XVII."[87] Yet, it is important to note that under GATS, countries have the option to opt-in and opt-out of certain commitments. So, countries may agree to liberalize one form of data flow while restricting another.
1995	Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)[88]	The TRIPS agreement includes rules on several forms of intellectual property, outlining the standards of IP protection, procedures for the enforcement of IPR, and procedures for the settlement of IPR disputes between countries. Within the context of the digital economy, the TRIPS agreement is used to protect intellectual property within the information and communications technology sector.
1996, expanded in 2015	The WTO's Information Technology Agreement (ITA)[89]	The 1996 ITA agreement resulted in the reduction of tariffs on IT goods. Currently, 81 members, which account for 97% of the world's trade in IT goods, have subscribed to the ITA agreement. In 2015, the agreement was expanded to include tariff reductions on new categories of IT products, with 54 members joining the updated agreement and reductions beginning in 2016.[90]

[84] "The General Agreement on Tariffs and Trade," WTO, July 1986, https://www.wto.org/english/docs_e/legal_e/gatt47.pdf.
[85] Amy Porges and Alice Enders, "Data Moving Across Borders: The Future of Digital Trade Policy," International Centre for Trade and Sustainable Development, World Economic Forum, E15 Expert Group on the Digital Economy, April 2018, https://www.tralac.org/images/docs/9554/data-moving-across-borders-the-future-of-digital-trade-policy-e15-initiative-april-2016.pdf.
[86] "General Agreement on Trade in Services," WTO, 1995, https://www.wto.org/english/docs_e/legal_e/26-gats.pdf.
[87] Amy Porges and Alice Enders, "Data Moving Across Borders."
[88] "Agreement on Trade-Related Aspects of Intellectual Property Rights," WTO, 1995, https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
[89] "Ministerial Declaration on Trade in Information Technology Products", WTO, December 19, 1996, https://www.wto.org/english/docs_e/legal_e/itadec_e.pdf.
[90] WTO, "Information Technology Agreement — an explanation," https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm.

Relevant Treaties and Legislation: Digital Trade		
Year	Treaty/Legislation	Summary
2016	The EU's General Data Protection Regulation (GDPR)[91]	The GDPR, which came into full effect in May 2018, is a legal framework that requires all platforms, regardless of location, to follow certain guidelines when collecting personal information from EU citizens. Because GDPR requires the world to comply with its requirements in order to access the EU digital market, the regulation has international trade ramifications. In a 2017 survey of 200 U.S. businesses, 68% of companies planned to invest between $1 and $10 billion to achieve GDPR compliance.[92] Given the costs of compliance, some companies have chosen to forgo the EU market altogether.
2016	The EU-U.S. Privacy Shield[93]	The EU-U.S. Privacy Shield provides U.S. and EU businesses with a mechanism to share data across borders while complying with EU data protection requirements.[94] Similarly, a Swiss-U.S. Privacy Shield was established for data transfers between the two countries since Switzerland is not a member of the EU. The European Commission declared that the privacy shield's data-sharing mechanism provided adequate protections for EU citizens, but this decision was invalidated by the Court of Justice of the European Union in 2020.[95] The Swiss-U.S. Privacy Shield was also invalidated by Switzerland's Federal Data Protection and Information Commissioner (FDPIC). However, these decisions did not relieve participants from their obligations under the privacy shield frameworks. In fact, over 5,000 businesses continue to use the EU-U.S. Privacy Shield and its Swiss counterpart today.[96]
2003, effective since 2004	U.S.-Singapore Free Trade Agreement (USSFTA)[97]	Chapter 14 of the USSFTA is dedicated to liberalizing e-commerce between the two countries. The section includes a provision to eliminate duties on "the importation or exportation of digital products by electronic transmission" and states that "A Party shall not accord less favorable treatment to some digital products than it accords to other like digital products."[98]

[91] "Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union*, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[92] PWC, "GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey," January 23, 2017, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.
[93] "Commission Implementing Decision (EU) 2016/1250," *Official Journal of the European Union*, July 12, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.
[94] Privacy Shield Framework, "Privacy Shield Overview," https://www.privacyshield.gov/Program-Overview.
[95] "Decision (EU) 2016/1250," *Official Journal of the European Union*.
[96] Privacy Shield Framework, "Privacy Shield List," https://www.privacyshield.gov/list.
[97] Office of the United States Trade Representative, *United States - Singapore Free Trade Agreement*, 2003, https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file708_4036.pdf.
[98] Office of USTR, *U.S.-Singapore FTA*, 154.

Relevant Treaties and Legislation: Digital Trade		
Year	Treaty/Legislation	Summary
2007, effective since 2012	US-South Korea Free Trade Agreement (KORUS FTA)[99]	The KORUS FTA includes provisions to facilitate e-commerce and information-sharing between the two countries. Chapter 15 of the FTA specifically deals with electronic commerce. It eliminates duties on digital products, prohibits the discriminatory treatment of digital products, and requires that both countries recognize electronic authentication and signatures.
2018, effective since July 2020	United States-Mexico-Canada Agreement (USMCA)[100]	Chapter 19 of the USMCA is dedicated to digital trade between the three countries. As in other FTAs, it includes provisions that prohibit duties and discriminatory treatment for digital products. Additionally, Chapter 19 covers online consumer protection, personal information protection, cross-border transfers of information, cybersecurity, and more. One noteworthy provision states that "no Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person."[101]

[99] Office of the United States Trade Representative, *The United States - Korea Free Trade Agreement*, 2007, https://ustr.gov/sites/default/files/uploads/Countries%20Regions/africa/agreements/pdfs/FTAs/South%20Korea%20FULL.pdf.
[100] Office of the United States Trade Representative, "Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text," July 5, 2020, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.
[101] Office of the United States Trade Representative, *Chapter 19 of the USMCA: Digital Trade*, 2020, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

ADDRESSING THE INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS (IPR)

The internet and digital technologies have been particularly challenging when it comes to the protection of present intellectual property rights (IPR)—*inter alia*, patents, copyrights, trademarks, and trade secrets. IPR are legal rights that grant exclusivity of use to inventors and authors for a limited time.

In recent years, IPR infringement has surged, mainly because digital technology makes counterfeiting and its distribution cheap, relatively easy, and hard to trace. Cyber-enabled theft of trade secrets has been particularly concerning for the United States, especially with regard to China. It is hard to know the exact figure for cyber-enabled IP loss, but it is likely a major part of the $600 billion in annual losses to Chinese theft of American IP, as estimated by the Commission on the Theft of American Intellectual Property Policy Recommendation (2018).[102]

While protecting IPR is critical to promote innovation, if IPR policies are too strict they could present obstacles to data flows and digital trade. To overcome this, U.S. law introduced the "fair use" doctrine that allows for unlicensed use of protected works under certain conditions. Similarly, there have been international efforts to define IP protections through IPR treaties since the nineteenth century.[103] The Berne Convention for the Protection of Literary

[102] Commission on the Theft of American Intellectual Property ("IP Commission"), Written Comments on Behalf of the Commission on the Theft of American Intellectual Property to the United States Trade Representative, 2018, https://www.nbr.org/wp-content/uploads/pdfs/publications/ustr_written_comments_301_tariffs-may2018.pdf. The IP Commission describes itself as an "independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academia, and politics."
[103] For a list of international IPR treaties that the U.S. is party to, see Tarlton Law Library: Jamail Center for Legal Research, "Intellectual Property," https://tarlton.law.utexas.edu/c.php?g=457743&p=3129119.

and Artistic Works (1886), was the first copyright multilateral convention. Nearly a century later, the international Patent Cooperation Treaty (PCT) was passed in 1970, providing states with a unified application procedure for patent protection. And, in 1995, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) was founded on these existing treaties, representing the most comprehensive international IPR treaty to date. It strived to balance private rights against broader public benefits and established a minimum required standard for protecting the intellectual property for the members of the WTO.

The TRIPS Agreement is comprehensive and covers all forms of IP including copyrights, trademarks, patents, and trade secrets. Like the GATS, it predates the internet era and has no direct reference to the digital ecosystem. However, it serves as a base for IPR provisions in ensuing trade negotiations, often identified as "TRIPS-plus." Digital Trade and U.S. Policy explains that "TRIPS incorporates the main substantive provisions of The World Intellectual Property Organization (WIPO) conventions by reference, making them obligations under TRIPS. WTO members were required to fully implement TRIPS by 1996, with exceptions for developing country members by 2000 and least-developed-country (LDC) members until July 1, 2021"[104]—for pharmaceutical patents, "the implementation period has been extended until January 1, 2033." [105]

"While protecting IPR is critical to promote innovation, if IPR policies are too strict they could present obstacles to data flows and digital trade."

The TRIPS provision on computer programs references the WIPO Berne Convention to treat computer programs' source and object code as literary works and, thus, protected. The TRIPS provision on data, as noted in its WTO overview, "clarifies that databases and other compilations of data or other material, whether in machine-readable form or not, are eligible for copyright protection even when the databases include data not under copyright protection."[106]

The WIPO is shaped by the TRIPS Agreement and serves as the administrator and primary forum for IPR issues in the digital realm. The WIPO "Internet Treaties"

[104] Congressional Research Service, Digital Trade and U.S. Trade Policy, 33.
[105] Congressional Research Service, Digital Trade and U.S. Trade Policy, 33.
[106] WTO, "Overview: the TRIPS Agreement," https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

consists of the Copyright Treaty and Performances and Phonograms Treaty. The Digital Trade and U.S. Trade Policy report summarizes the treaties, writing that they "clarify that existing rights continue to apply in the digital environment, to create new online rights, and to maintain a fair balance between the owners of rights and the general public."[107] It provides for legal protection against circumventing Technological Protection Measures (TPMs), including encrypting, as well as removing or modifying the encoded rights management information (RMI), which makes it possible to trace the usage of the information. National governments are left to work out the legal details for the internet service provider (ISP) obligations. The WIPO Internet Treaties' implementation in the United States takes place through the Digital Millennium Copyright Act (DMCA) of 1998 (H.R. 2281) that offers "safe harbor" to ISPs that "unknowingly" transmit copyrighted information.[108]

Other important agreements include the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (known as the Madrid Protocol) (joined by the U.S. in 2003), and the Anti-Counterfeiting Trade Agreement (ACTA) (adopted by the U.S. in 2011).[109]

The Digital Trade and U.S. Trade Policy report also notes the significance of the new EU Directive on Copyright in the Digital Single Market adopted on April 17, 2019, to update copyright laws for the internet era and provide a balanced and fair content marketplace.[110] Their directive on "neighboring rights" reimburses news publishers and journalists for the online usage of content. [111] Google and other news aggregation platforms must obtain licenses from content providers to showcase content less than two years old. In the absence of a license, agreement platforms must make best efforts to remove copyrighted materials once notified, though only older and more established platforms are subject to the requirements. While the U.S. publishing industry supports the new rules, content aggregators have expressed concerns about degraded market efficiency.

[107] Congressional Research Service, Digital Trade and U.S. Trade Policy, 33.
[108] Electronic Frontier Foundation, "Digital Millennium Copyright Act," https://www.eff.org/issues/dmca.
[109] Tarlton Law Library, "Intellectual Property."
[110] Congressional Research Service, Digital Trade and U.S. Trade Policy, 17.
[111] Congressional Research Service, Digital Trade and U.S. Trade Policy, 17.

Relevant Treaties and Legislation: Intellectual Property Rights		
Year	Treaty	Summary
1995	Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)[112]	Article 10.1 of the TRIPS Agreement, as noted in its WTO overview, "provides that computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)."[113] And, Article 10.2 "clarifies that databases and other compilations of data or other material shall be protected as such under copyright even where the databases include data that as such are not protected under copyright."[114]
1886, revised in 1971	Berne Convention for the Protection of Literary and Artistic Works[115]	The Berne Convention lays the foundation of international copyright law, ensuring the protection of works and the rights of authors. It is the predecessor of the World Intellectual Property Organization (WIPO). Today, the Berne Convention is applied to the digital environment through the WTO TRIPS Agreement and the WIPO Copyright Treaty (WCT).
1996, effective since 2002	The WIPO "Internet Treaties"[116]	The WIPO "Internet Treaties" consist of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, which together outline international IPR standards for works in the digital environment.
1996, effective since 2002	The WIPO Copyright Treaty[117]	Under the WIPO Copyright Treaty, computer programs and compilations of data or databases are protected as intellectual property. The treaty also outlines rights granted to the authors of computer programs and database – the right of distribution, the right of rental, and the right of communication to the public.[118]
1996, effective since 2002	The WIPO Performances and Phonograms Treaty[119]	The WIPO Performances and Phonograms Treaty deals with the rights of performers and producers of phonograms in the digital environment. Both performers (actors, singers, musicians, etc.) and producers of phonograms (any person or legal entity that produces a fixation of sound) are granted the right of reproduction, the right of distribution, the right of rental, and the right of making available.[120] Additionally, performers are granted moral rights, meaning they can object to any modification of their work that would affect their reputation. Under the Treaty, performances and phonograms must be protected for at least 50 years.

[112] WTO, "Agreement on Trade-Related Aspects of Intellectual Property Rights," 1995, https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
[113] WTO, "Overview: the TRIPS Agreement," https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.
[114] WTO, "Overview: the TRIPS Agreement."
[115] "Latest text of Berne Convention (1971 Paris Act plus Appendix)," completed September 9, 1996, final revision July 24, 1971, https://global.oup.com/booksites/content/9780198259466/15550001.
[116] WIPO, "WIPO Internet Treaties," https://www.wipo.int/copyright/en/activities/internet_treaties.html.
[117] "WIPO Copyright Treaty (WCT)," 1998, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_226.pdf.
[118] WIPO, "Summary of the WIPO Copyright Treaty (WCT) (1996)," https://www.wipo.int/treaties/en/ip/wct/summary_wct.html.
[119] "WIPO Performances and Phonograms Treaty (WPPT)," 1996, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_227.pdf.
[120] WIPO, "Summary of the WIPO Performances and Phonograms Treaty (WPPT) (1996)," https://www.wipo.int/treaties/en/ip/wppt/summary_wppt.html.

Relevant Treaties and Legislation: Intellectual Property Rights		
Year	Treaty	Summary
1998, effective since 2000	U.S.' Digital Millennium Copyright Act (DMCA)[121]	The DCMA implements the WIPO Internet Treaties into U.S. law. It includes two controversial sections: the "anti-circumvention" provisions (section 1201), which "bar circumvention of access controls and technical protection measures" and the "safe harbor" provisions (section 512), which "protect service providers who meet certain conditions from monetary damages for the infringing activities of their users and other third parties on the net."[122] In other words, anti-circumvention aims to prevent the piracy of digital goods, but can unintendedly stifle free expression and scientific research.[123] On the other hand, "safe harbor" offers immunity from copyright infringement liability to platforms so long as they take down infringing content once they are notified.
1989, effective since 1996	The Madrid Protocol[124]	The system established by the Madrid Protocol registers and manages trademarks worldwide. Under the Madrid System, individuals or legal entities may apply for an international trademark that is protected in all 106 of the Contracting Parties.
2011, yet to be ratified	Anti-Counterfeiting Trade Agreement (ACTA)[125]	The ACTA is a multilateral treaty that would establish a new legal framework and governing body on intellectual property rights, with particular emphasis on preventing copyright infringement on the internet. It was originally signed by the U.S., Australia, Canada, Japan, Morocco, New Zealand, Singapore, and South Korea in 2011, later joined by Mexico and the European Union in 2012. Only Japan has formally ratified the agreement so far. Many believe that ACTA could pose a threat to users' freedom of speech, privacy and civil liberties. The secretive nature of negotiations has also been criticized, as it excluded input from policymakers and citizens.[126]

[121] U.S. Congress, Digital Millennium Copyright Act, October 28, 1998, https://www.copyright.gov/legislation/pl105-304.pdf.
[122] Electronic Frontier Foundation, "Digital Millennium Copyright Act
," https://www.eff.org/issues/dmca.
[123] Electronic Frontier Foundation, "Unintended Consequences: Fifteen Years under the DMCA," March 2013, https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca.
[124] "Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks," Adopted at Madrid on June 27, 1989, https://www.wipo.int/edocs/lexdocs/treaties/en/madridp-gp/trt_madridp_gp_004en.pdf.
[125] "Anti-Counterfeiting Trade Agreement," 2011, https://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf.
[126] Electronic Frontier Foundation, "Anti-Counterfeiting Trade Agreement," https://www.eff.org/issues/acta.

Relevant Treaties and Legislation: Intellectual Property Rights		
Year	Treaty	Summary
2019	The EU Directive on Copyright in the Digital Single Market[127]	This EU directive updates copyright rules to more effectively address the issue of copyright infringement in the digital environment. It is important to note that EU directives are not automatically implemented in member states, they must be "transposed" into national law. The most controversial aspects of the new EU Copyright Directive are Article 17 (formerly Article 13) and Article 15 (formerly Article 11). Article 17 would require online platforms to proactively identify and take down infringing content, which would lead to the use of automated copyright filters and, thus, censorship.[128] Article 15, known colloquially as "the link tax," gives news companies the right to charge for links or "snippets" of their articles.[129] It is intended to allow companies to seek remuneration from Big Tech platforms like Google and Facebook that collect and display headlines and snippets of news stories. Yet, the provision does not outline any protections for small platforms and blogs that repurpose news links, and it also allows news companies to ban certain platforms from linking their content altogether, significantly hampering freedom of expression and online dialogue.

[127] "Directive (EU) 2019/790 of the European Parliament and of the Council," Official Journal of the European Union, April 17, 2019, https://eur-lex.europa.eu/eli/dir/2019/790/oj.
[128] Christoph Schmon, "EFF to EU Commission on Article 17: Prioritize Users' Rights, Let Go of Filters," Electronic Frontier Foundation, September 11, 2020, https://www.eff.org/deeplinks/2020/09/eff-eu-commission-article-17-prioritize-users-rights-let-go-filters.
[129] Cory Doctorow, "The European Copyright Directive: What Is It, and Why Has It Drawn More Controversy Than Any Other Directive In EU History?," Electronic Frontier Foundation, March 19, 2019, https://www.eff.org/deeplinks/2019/03/european-copyright-directive-what-it-and-why-has-it-drawn-more-controversy-any.

ASSURING CYBERSECURITY

When the U.S. Department of Defense's Advanced Research Projects Agency (ARPA) initiated the internet in 1960, it could hardly have imagined what its creation would entail. Once it became the public internet in 1989, the network created a new world and became the dominant feature of twenty-first century society, commerce, and national security—one that led to immense strength but, paradoxically, also great vulnerability.

Neither the government nor the private sector anticipated the speed of this technological revolution and the challenges it would pose. As a result, the internet still operates on protocols that have their origins in the 1960s and that some perceive to be inherently vulnerable. These vulnerabilities are exploited for crime, espionage, and warfare. Cybercrime alone is predicted to cost the global economy $6 trillion by 2021. Cyberattacks threaten to destabilize not only business operations and supply chains but also financial and communications infrastructure, national security, privacy, trade, and commerce.[130]

As for espionage and cyberwarfare, the costs are hard to estimate, but these practices are widespread. At the turn of the twenty-first century, governments, including the U.S. government, realized that they could use their new cyber capabilities to go beyond spying. They could covertly insert code or information in order to influence, disrupt, or destroy.

"Cybercrime alone is predicted to cost the global economy $6 trillion by 2021."

The list of operations is long, including cyberattacks between the United States and Iran; Israel and Iran; Russia against Estonia, Georgia, and Ukraine; and so on. Particularly salient were Russian interferences in the U.S. democratic process and the subsequent American retaliation against the Russian Internet Research Agency, Iran's data-wiping attack on Saudi Aramco, and North Korea's attack on Sony Pictures as well as its recent global banking heist, along with many more. Worse, there is the possibility that the states conducting cyber offensives may lose control, inadvertently damaging third parties. There is also the ever-

[130] Congressional Research Service, Digital Trade and U.S. Trade Policy, 19.

present risk of miscalculation and human error from which escalation can ensue.

States involved in espionage, like criminals involved in crime, try to hide their identities or at least maintain plausible deniability. Yet, when attribution is possible, nations can prosecute those responsible for cybercrimes but not for espionage—such activities remain the murky domain of clandestine operations.

Even when a no-espionage agreement is achieved, it is often ineffective. The 2015 Sino-American agreement on cyber-security and trade secrets is illustrative. It pledged that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[131] The G-20's November 2015 communiqué discussing the information and communication technology (ICT) environment, explains "just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[132] Section 301 Investigations into China's alleged infringements of U.S. IPR began in August 2017, and by December 2018, U.S. Assistant Attorney General John C. Demers announced that over the previous seven years, 90 percent of Justice Department's espionage cases and two-thirds of trade secrets cases were connected or attributable to China.[133] This led to a greater escalation of the trade war, with tariffs increasing on both sides.

By contrast, in dealing with non-state-sponsored cybercrime, countries enter multilateral and bilateral treaties and agreements as well as public-private partnerships and engage in setting norms. Still, it is not an easy ride, for there are many conflicting beliefs, including differing visions of the internet—ranging from an open and free market to authoritarian and controlled—and the elusive balance between cybersecurity on the one hand and privacy, anonymity, and encryption on the other.

[131] The White House under President Barack Obama, "Fact Sheet: President Xi Jiping's State Visit to the United States," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[132] Daniel Paltiel, "G20 Communiqué Agrees on Language to Not Conduct Cyber Economic Espionage," CSIS, November 16, 2015, https://www.csis.org/blogs/strategic-technologies-blog/g20-communiqu%C3%A9-agrees-language-not-conduct-cyber-economic.
[133] John C. Demers, "Statement of John C. Demers Assistant Attorney General, National Security Division U.S. Department of Justice Before the Committee on the Judiciary", U.S. Department of Justice, presented on December 12, 2018, https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20Demers%20Testimony.pdf.

Yet, despite these obstacles, critical treaties have been reached. The Convention on Cybercrime of the Council of Europe (2001) is one of the first international treaties on cybercrime that is legally enforceable since 2004.[134] It establishes common standards for inspection and facilitates criminal justice collaboration for its forty-seven member countries and sixty-eight signatories, including the United States.[135] It is not a static treaty and can be updated to meet evolving needs, and it is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.

"... it is not an easy ride, for there are many conflicting beliefs, including differing visions of the internet—ranging from an open and free market to authoritarian and controlled—and the elusive balance between cybersecurity on the one hand and privacy, anonymity, and encryption on the other."

President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace at the United Nations Internet Governance Forum (IGF) in 2018. As noted by the Digital Watch Observatory, it expands the Tunis Agenda's definitions for states and stakeholders while also reinforcing UN guidance about international law's jurisdiction in cyberspace.[136] The Budapest Convention is also recognized as a critical instrument to fight against cybercrime, while the private sector is held responsible for the security of digital products. The DiploFoundation's Director of E-diplomacy and Cybersecurity Programmes, Vladimir Radunovic, summarizes the Call aptly, writing that it focuses on "broad digital cooperation and capacity-building" and "safeguard[s] against damage to the general availability or integrity of the public core of the Internet, foreign intervention in electoral processes, ICT-enabled theft of intellectual property for

[134] Council of Europe, "Budapest Convention and related standards," 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[135] Allison Peters and Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime," Journal of National Security Law & Policy, no. 10:487 (2020): 499-500, https://jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf.
[136] Geneva Internet Platform Digital Watch Observatory, "Macron Launches Paris Call for Trust and Security in Cyberspace," https://dig.watch/updates/macron-launches-paris-call-trust-and-security-cyberspace.

competitive advantage, and non-state actors 'hacking-back'."[137]

He also notes that the Paris Call had "strong initial support from hundreds of signatories, including leading tech companies and many governments. Yet, the USA, Russia, and China are missing from the roll."[138] Since 2019, Russia, with the help of China and other mostly authoritarian countries, has pushed the UN for a new global cybercrime treaty to replace the Budapest Convention. The draft offers broader global cooperation on cybercrime, but the proposed treaty's vague language raises several human rights questions.[139]

There are also critical bilateral treaties and agreements to facilitate cooperation among countries in cybercrime investigations and prosecutions. Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAs), while not necessarily focused on cybercrime, have been very useful in cybercrime investigations, usually enumerating the different evidentiary items that opposing sides must produce.[140]

As of 2018, the United States had entered MLAAs with sixty-five other nations, the EU, and China. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[141] was passed in 2018 by Congress, summarized by Third Way as allowing "the United States to enter into negotiations for executive agreements with other nations who can meet certain privacy and civil liberties standards in order to facilitate cross-border data sharing directly between U.S. tech companies and foreign governments" (aimed at reducing the backlog and delays).[142]

The United States is also a signatory to over one hundred extradition treaties, which set the rules for surrendering individuals to another country for crimes committed in that country. The problem is that the most problematic countries are not signatories. The dual criminality condition of these agreements requires

[137] Vladimir Radunovic, "At the table with the Paris Call for Trust and Security in Cyberspace," DiploFoundation, December 19, 2018, https://www.diplomacy.edu/blog/table-paris-call-trust-and-security-cyberspace.
[138] Radunovic, "Paris Call."
[139] Joyce Hakmeh and Allison Peters, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet," Council on Foreign Relations, January 13, 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.
[140] Allison Peters and Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime," Third Way, May 27, 2020, https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime.
[141] U.S. Department of Justice, Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019, https://www.justice.gov/opa/press-release/file/1153446/download.
[142] Allison Peters and Anisha Hindocha, "US Global Cybercrime Cooperation: A Brief Explainer," Third Way, June 26, 2020, https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer.

that an offense be deemed criminal by the laws of both countries in order for a person to be extradited. This creates challenges for advanced countries facing crime from countries with outdated national cybercrime laws. Another mechanism is the INTERPOL, the world's largest police organization. It facilitates information sharing and assistance in criminal investigations. Through its red notice system, countries can circulate notices for cybercriminals that are wanted for extradition in order to locate and arrest the perpetrators.[143]

In addition to these formal agreements, there are many international organizations and forums that facilitate informal cooperation. Their role is particularly important in facilitating communications between the countries where no formal treaties exist or where diplomatic relationships are not strong. One key organization is the United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ), which was established in 1992 and is the UN's principal policy-making body on all matters of crime prevention and criminal justice, including cybercrimes.

The CCPCJ also oversees the UN Office on Drugs and Crime (UNODC), which educates countries on cybercrime. It is also the preparatory body for the UN Crime Congress—a high-level meeting of government officials held every five years to discuss important criminal matters, where cybercrime has been a primary focus recently.[144]

The Group of Seven (G7)'s 24/7 Cybercrime Network brings together the leaders of developed countries, including the United States.[145] The network, which includes more than seventy nations, sets up points of contact for immediate requests for preserving digital evidence, including in cybercrime cases. The Global Forum on Cyber Expertise (GFCE) is a multi-stakeholder forum that serves as a clearinghouse, promotes global cooperation on cyber capacity building, and shares data and expertise on cybercrime.[146]

There are increasing calls to establish global norms to guide responsible nation-state behavior in cyberspace. The fourth UN Group of Governmental Experts on

[143] Jonathan Masters, "What is Extradition?," Council on Foreign Relations, January 8, 2020, https://www.cfr.org/backgrounder/what-extradition.
[144] United Nations Congress on Crime Prevention and Criminal Justice, "About," https://www.unodc.org/congress/en/about.html.
[145] For more information on the 24/7 Cybercrime Network, see Chris Ott, "What You Should Know About The 24/7 Cybercrime Network," Davis Wright Tremain LLP, June 28, 2018, https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf.
[146] Global Forum on Cyber Expertise (GFCE), https://thegfce.org/.

Developments in the Field of Information and Telecommunications in the Context of International Security's 2015 report agreement is an attempt in this direction. It establishes governing principles and rules of conduct in cyberspace for nation-states.[147] The G7 Declaration on Responsible States Behavior in Cyberspace (called the Lucca Declaration), issued in 2017, requires that nation-states consider cooperative measures to address cyber threats. The United States is a member of these forums, and the International Cyberspace Policy articulated in the Cyber Diplomacy Act of 2019 (H.R. 739) was a direct call from Congress demanding the State Department step up its leadership in this area.

"There are increasing calls to establish global norms to guide responsible nation-state behavior in cyberspace."

[147] Peters and Hindocha, "US Global Cybercrime Cooperation."

Cybersecurity: Relevant Treaties, Legislation, and Documents		
Year	**Document**	**Summary**
2001, effective since 2004.	The Council of Europe's Convention on Cybercrime[148]	The Convention on Cybercrime, commonly referred to as the Budapest Convention, "is the only legally binding international treaty that sets common standards on investigations and criminal justice cooperation on cybercrime."[149] It applies to the Council of Europe's 47 member countries and the treaty's 68 signatories, including the United States.
July 2015	The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Report[150]	The report outlines "existing and emerging threats" and establishes "norms, rules and principles for the responsible behavior of States" in cyberspace.[151] The document also calls on states to voluntarily adopt "confidence-building" measures, including "cooperative mechanisms between relevant agencies to address ICT security incidents" and "a national computer emergency response team and/or cybersecurity incident response team."[152]
September 2015	U.S.-China Cyber Agreement[153]	Under the agreement, both countries pledged "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[154] Additionally, both countries agreed to establish "a high-level joint dialogue mechanism on fighting cybercrime and related issues."[155]

[148] "Convention on Cybercrime," European Treaty Series - No. 185, Council of Europe, November 23, 2001, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.
[149] Peters and Jordan, "Countering the Cyber Enforcement Gap."
[150] United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations Digital Library, July 22, 2015, https://digitallibrary.un.org/record/799853?ln=en#record-files-collapse-header.
[151] United Nations General Assembly, "Report," 3.
[152] United Nations General Assembly, "Report," 9-10.
[153] The White House under President Barack Obama, "Fact Sheet: President Xi Jiping's State Visit to the United States," September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[154] The White House, "Fact Sheet."
[155] The White House, "Fact Sheet."

Cybersecurity: Relevant Treaties, Legislation, and Documents		
Year	**Document**	**Summary**
November 2015	The G-20 Communiqué[156]	Paragraph 26 of the communiqué affirms that " no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[157] Though the agreement is not legally binding, it represents a commitment to responsible state behavior in cyberspace.
2017	G7 Declaration on Responsible States Behavior in Cyberspace (Lucca Declaration)[158]	The Lucca Declaration emphasizes that certain cyber activities can amount to the use of force and may even be considered an armed attack. Additionally, the declaration calls on "States to publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible in order to improve transparency and give rise to more settled expectations of State behavior."[159] It references the norms of State behavior outlined in the 2015 G-20 Communiqué.
2018	Paris Call for Trust and Security in Cyberspace[160]	The Paris Call is a commitment that invites nation-states and cyberspace actors to work together to ensure the safety of citizens and infrastructure. The call is based on nine common principles: protect individuals and infrastructure, protect the internet, defend electoral processes, defend intellectual property, non-proliferation, lifecycle security, cyber hygiene, no private hack-back, and international norms.[161] It is currently supported by 78 nation-states, 29 public authorities and local governments, 349 organizations and members of civil society, and 648 companies and private sector entities.[162] China, Russia and the U.S. have not signed onto the call.

[156] G20 Turkey 2015, "G20 Leaders' Communiqué," Antalya Summit, 15-16 November 2015, http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.
[157] Daniel Paltiel, "G20 Communiqué."
[158] "G7 Declaration on Responsible States Behavior in Cyberspace," Lucca, April 11, 2017, https://ccdcoe.org/uploads/2018/11/G7-170411-LuccaDeclaration-1.pdf.
[159] "G7 Declaration on Responsible States Behavior in Cyberspace," 3.
[160] "The Paris Call for Trust and Security in Cyberspace", November 12, 2018, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.
[161] Paris Call, "The 9 principles," https://pariscall.international/en/principles.
[162] Paris Call, https://pariscall.international/en/.

Cybersecurity: Relevant Treaties, Legislation, and Documents		
Year	**Document**	**Summary**
2018	The U.S.' Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[163]	This act is summarized by Third Way as allowing the United States to enter into negotiations for executive agreements with other nations who can meet certain privacy and civil liberties standards in order to facilitate cross-border data sharing directly between U.S. tech companies and foreign governments (aimed at reducing backlog and delays).[164] With regard to cybercrime, the CLOUD Act facilitates investigative procedures for both U.S. and foreign governments by allowing them to access tech companies' electronic information. This is critical to the investigation of serious crimes "ranging from terrorism and violent crime to sexual exploitation of children and cybercrime."[165]
2019	The U.S.' Cyber Diplomacy Act of 2019[166]	The International Cyberspace Policy outlined in Section 4 of this act states that the President shall pursue several cybersecurity objectives, including "securing and implementing commitments on responsible country behavior in cyberspace."[167] The act also establishes an Office of International Cyberspace Policy within the State Department.

[163] U.S. Congress, "Clarifying Lawful Overseas Use of Data Act," S.2383, February 6, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[164] Peters and Jordan, "Countering the Cyber Enforcement Gap."
[165] U.S. Department of Justice, The Purpose and Impact of the CLOUD Act, 2.
[166] U.S. Congress, "Cyber Diplomacy Act of 2019," H.R. 739, January 24, 2019, https://www.congress.gov/bill/116th-congress/house-bill/739/text#toc-HF69B2046ABEB4D71A8C145F6BFBADD92.
[167] U.S. Congress, "Cyber Diplomacy Act of 2019."

CYBER DIPLOMACY

Information technology has always affected diplomacy—witness the contrast between the eighteenth century, when diplomats could negotiate in foreign capitals unencumbered by instructions from home for weeks at a time, and the digital present when capitals can communicate with each other instantaneously. Diplomats abroad, especially American ones, now inhabit bunkers that, to varying degrees, limit face-to-face contact with the foreigners they are meant to court. (However, the Wikileaks release of State Department cables in 2010 was the best advertisement for the U.S. foreign service, showing diplomats doing their job, talking with foreigners of interest and often reporting those conversations in surprisingly graceful prose!)

Looking to the future, the ubiquity of data and artificial intelligence (AI) will transform diplomacy. That transformation might be conceived of in three categories—data in diplomacy, diplomacy for data, and data for diplomacy, or, respectively, the use of data to advance or constrain diplomacy, negotiations about how data will be handled across borders, and data as a way to enhance diplomatic capability.[168] The second category, diplomacy for data, has run through this entire paper, but it is worth saying a word about the other two.

Concerning data in diplomacy, formal diplomacy has long distinguished between Track I discussions between government officials, and Track II discussions involving a wider set of experts or stakeholders outside the government. Nations often resort to Track II when formal Track I negotiations are not available or are deemed a step too far. Recently, the term "Track 1.5" has become popular, referring to governments' discreet participation through a third party or organization.

The growing availability of data will increase both the number of non-governmental actors who influence formal diplomacy and the purposes for which that data is employed. Imagine, for instance, if ethnic cleansing in the former Yugoslavia during the 1990s had occurred in the presence of ubiquitous cellphone cameras. Fresh gravesites, such as those in the massacre at Srebrenica, would have been documented immediately for the world to see. More data for more participants will

[168] Andy Boyd et al., "Data Diplomacy," Science & Diplomacy, AAS Center for Science Diplomacy, June 24, 2019, https://www.sciencediplomacy.org/article/2019/data-diplomacy.

"The growing availability of data will increase both the number of non-governmental actors who influence formal diplomacy and the purposes for which that data is employed."

make formal diplomacy messier and less predictable—witness the 2013 disclosure by Edward Snowden of National Security Agency surveillance programs, which he justified as whistle-blowing and which did, in the end, play some role in the public pressure that lead to the GDPR.

In the third category, data for diplomacy, data experts, and increasing amounts of data will create new relationships and thus new opportunities for diplomacy. In principle, this should be a great boon for the effort to adapt the existing international architecture to the emerging world. A current example is the UN Global Pulse, which bridges the public-private divide by seeking to use big data's best practices for the benefit of international development and humanitarian relief; the initiative even includes a volunteer program for data scientists.

LOOKING FORWARD

As this paper has laid out in painstaking detail, data governance happens in a patchwork of settings. As an example, privacy is not regulated by a singular American law, let alone the virtual domain more broadly.[169] Even at just the federal level, a host of organizations and laws are at play.

The Federal Trade Commission Act (1914) bans unfair or deceptive commercial practices, and the FTC is the chief federal agency on privacy. The Electronic Communications Privacy Act (1986) safeguards certain wire, oral, and electronic communications, and the Computer Fraud & Abuse Act (1986) prohibits unauthorized access to a computer. The Children's Online Privacy Protection Act (1998) requires parental consent before collecting, using, or disclosing personal information from minors under the age of thirteen. It also, as noted in a Reuters legal article, "requires websites to post an online privacy policy, collect only necessary personal information, and maintain reasonable security measures."[170]

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (the CAN-SPAM Act, 2003) provides guidelines for the operation of commercial emails. The Financial Services Modernization Act (1999) regulates the personal data collection practices of financial institutions. Finally, the Fair and Accurate Credit Transactions Act (2003) increases consumers' protection from identity theft.[171] As some observers put it, "Today's patchwork of privacy laws and industry self-regulation lacks transparency and coherence: the combination drives up the cost of innovation and doesn't go far enough to encourage healthy competition or to protect the billions of people worldwide who now rely on the products and services tech companies produce."[172]

Yet, the challenge is global, not national, for the combined impact of big data, artificial intelligence (AI), machine learning (ML), and the Internet of things (IoT) is driving an escalation in geopolitical tension. Today, data ownership has become critical to the balance of power, and the impact is exacerbated by the prospect of ML that

[169] Thomson Reuters, "Internet Privacy Laws - how your personal information is protected online," https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online.
[170] Thomson Reuters, "Internet Privacy Laws."
[171] Thomson Reuters, "Internet Privacy Laws."
[172] Quest and Charrie, "The Right Way to Regulate the Tech Industry."

mobilizes big data beyond human capacity and by its potential to generate intellectual property. Unlike the tangible and production-based economy, which encourages globalization and free trade, the intangible data-economy seems to favor protectionism. The collective impact is redefining geopolitics with no precedent, as manifested in data balkanization, AI nationalism, lawfare, and even the potential for "splinternets." The combination is posing dangerous threats to global stability and order, and the United States could find itself on the outside looking in.

One starting point would be for countries to create a single regulator for the tech industry, and to decide what is to be regulated and what not, and how tech companies will be incorporated into the regulatory framework. The goal would be to protect individuals with consistent, comprehensive rules for data privacy, while still promoting innovation. The system would be risk-based, focusing on companies and actions that put the most people at risk. Ideally, regulators would work closely with the companies to address emerging risks as quickly and efficiently as possible.

Moving toward a global agreement on how to balance open data flows with other national interests, namely cybersecurity and privacy, will be critical in maintaining trust in the digital world and sustaining international trade.[173] A host of forums and organizations are debating how to find adequate mechanisms capable of achieving the right balance. Chief among these forums are:

- **The G-20**: an influential venue that establishes common principles. In 2017, the forum created the Digital Economy Task Force (DETF), which in turn identified the requirements for healthy discussions and made several recommendations.[174] During the G-20 meeting in Japan, members agreed to resolve differences through consultation and to face challenges together. New rules are being considered for free data flows across borders worldwide, and the "Osaka Track" framework was launched to protect data privacy.[175]
- **The Organization for Economic Cooperation and Development (OECD)**: another important forum that addresses the digital economy. Its reports on digital trade include one that

[173] Congressional Research Service, Data Flows, Online Privacy, and Trade Policy, March 11, 2019, https://fas.org/sgp/crs/row/R45584.pdf.
[174] G-20 Argentina, "The G20 confirms the importance of the digital economy for global development," August 24, 2018, https://g20.argentina.gob.ar/en/news/g20-confirms-importance-digital-economy-global-development.
[175] Bi Ran, "Graphics: Key achievements of G20 Osaka summit," CGTN, July 1, 2019, https://news.cgtn.com/news/2019-06-29/G20-Osaka-Summit-concludes-in-Japan--HUUcyBdg9G/index.html.

assesses[176] the digital development of each OECD country and another on bridging the digital gender divide.[177] The OECD Global Forum on Digital Security for Prosperity focuses, as its name implies, on governing those security issues.

- **The Asian Pacific Economic Cooperation (APEC)**: an important regional forum that shares practices and establishes principles for issues that concern countries whose digital economies are less developed. The APEC Cross-Border Privacy Rules (CBPR) System is a very popular government-backed data privacy certification that implements the APEC Privacy Framework (2005, updated in 2015). APEC is voluntary, but it has served as a useful forum for incubating agreements.[178]

These powerful forums have already begun addressing the challenges that the digital age poses for our global society. Yet, judging by the chaotic status of geopolitics today and the number of abandoned agreements over the last decade, they are not delivering. As our detailed study of global agreements and their legislative foundations illustrates, achieving concurrence is often a very slow process that involves complex negotiations among multiple actors with competing interests, conflicting visions, and different values. Besides, treaties rest on an evolving body of legislation that is aggregated with time. This tendency to look back to find a solution for current or emerging problems has proven successful for most of recent history. However, old solutions are mismatched to disruptive, dynamic, and unpredictable cyber technologies. The result is years of slow and complex negotiations that seek to find solutions to new problems through an outdated lens. Current debates pose these questions harshly: How do governments apply publisher legislation to cyber platforms? How will antitrust laws apply to tech giants?

Meanwhile, despite receiving a great deal of attention in the media, big data is hardly touched upon in the global governance debate. Often, data is discussed in relation to privacy, but big data is almost always about multiple datasets and in many cases has little to do with personal data. Big data is also discussed in terms of volume, variety, and velocity, but the impact of its dynamic nature is hardly considered. Too little attention is given to the interplay between big data, ML, AI, and the ability of

[176] OECD, Key Issues for Digital Transformation in the G20, Berlin, Germany, January 12, 2017, https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf.
[177] OECD, Bridging the Digital Gender Divide: Include, Upskill, Innovate, 2018, http://www.oecd.org/sti/ieconomy/bridging-the-digital-gender-divide.pdf.
[178] APEC, "What is the Cross-Border Privacy Rules System?," April 15, 2019, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

algorithms to generate and test hypotheses, let alone broader issues about the nature of human-machine relationships. Big data is removing old borders and constructing new ones in ways not well understood. We need forums that engage innovators, thought leaders, and legislators in frank discussions that go beyond current divisions over narrow, often parochial perspectives. At stake is our common future and how we would like to shape it.

The problem is that the digital age presents geopolitical and philosophical problems beyond the capabilities of the existing global architecture and its institutions. They remain inadequate in dealing with the cross-border, complex, and opaque nature of big data. The unhappy geopolitical context calls for an urgent Bretton Woods-style gathering to ensure that the most transformative technologies of our time do not spiral out of control and create a world order we will come to regret.

The Digital-20 (D-20): It is a new initiative launched by the Global Techno-Politics Forum aiming to fill this void and to function as a bridge between the existing global architecture and the new geopolitical context. The D-20 would build upon the important work and the initiatives led by the Bretton Woods institutions and the founding internet organizations and other think tanks in establishing international codes and standards as well as demonstrating leadership. Still in its infancy, D-20 in many respects is modeled on the G-20, with the new group broadening the scope of dialogue to new stakeholders and digitally mature eco-systems, and shifting the focus to the key geopolitical challenges caused by the emerging digital technologies. As an autonomous group with no executive power and no binding decisions, its primary impact lies in creating trust and peer-to-peer intimacy among members as they develop a shared diagnosis of potential problems and a common analytical framework in small, intimate convenings. Building on this trust, the D-20 will strive to produce actionable and measurable outcomes.

ABOUT THE AUTHORS

Gregory F. Treverton

Gregory F. Treverton is co-founder and chairman at the Global TechnoPolitics Forum. He served as chairman of the National Intelligence Council from September 2014 to January 2017. Currently, he is a senior adviser with the Transnational Threats Project at the Center for Strategic and International Studies (CSIS) and a professor of the practice of international relations and spatial sciences at the University of Southern California. Earlier, Treverton directed the RAND Corporation's Center for Global Risk and Security and served as associate dean of the Pardee RAND Graduate School. He has also taught at Harvard and Columbia universities, was a senior fellow at the Council on Foreign Relations, and served as deputy director of the International Institute for Strategic Studies in London. Treverton worked in government on the staff of the first Senate Select Committee on Intelligence, on the National Security Council staff, and as vice chair of the National Intelligence Council. He holds an AB summa cum laude from Princeton University and an MPP (Master's in Public Policy) and PhD in economics and politics from Harvard.

Pari Esfandiari

Pari Esfandiari is co-founder and president of Global TechnoPolitics forum. She is a member of the At-Large Advisory Committee (ALAC) at ICANN and serves as Nonresident Senior Fellow at the Atlantic Council's GeoTech Center. Esfandiari is a serial entrepreneur, internet pioneer, and sustainable development executive. Her extensive international background includes leadership, advisory, and investment positions with organizations and corporations in China, Europe, the Middle East, and the United States. Esfandiari has worked across diverse industries ranging from FinTech and e-commerce to sustainability and smart cities. She has a doctorate from Oxford Brookes University in the sustainability business and is an avid environmentalist.

GLOBAL TECHNOPOLITICS FORUM LEADERSHIP

Chairman

Gregory F. Treverton

President

Pari Esfandiari

Board of Advisors

Philip Chase Bobbitt

David Bray

Thomas A. Campbell

Shelby Coffey

Shanta Devarajan

C. Bryan Gabbard

Nancy K. Hayden

Jim Herriot

Molly Jahn

Spencer Kim

Robert Klitgaard

Ronald Marks

Barry A. Sanders

Rod Schoonover

Davide Strusani

Peter Vale

John Walcott

James F. Warren

David K. Young

The Global TechnoPolitics Forum is a 501(C)(3) nonprofit educational organization with a mission to shape the public debate and facilitate global coordination at the intersection of technology and geopolitics. It achieves this mission through: convenings, research, and community building.

© 2020 The Global TechnoPolitics Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global TechnoPolitics Forum, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to Global TechnoPolitics Forum.

www.TechnoPolitics.org
ISBN: 978-1-7362034-0-8
info@technopolitics.org
Tel: +1.202.735.1415