The proliferation of internet users has shifted the center of gravity of the internet away from the United States, making it more global and broadly distributed among emerging and mature economies. As national and subnational regulators around the world attempt to expand sovereign control over the internet, its future as a free, open, and interoperable platform is under threat. A bipartisan approach in Washington is critical for U.S. leadership in digital governance. This brief maps out a strategy for effective and sustained multilateral engagement on these issues.

 INTRODUCTION AND BACKGROUND

Over the past three decades, the center of gravity of internet users has shifted away from the United States and is now more globally distributed among emerging and mature economies. Half of all internet users reside in the developing world. China, India, and Indonesia alone are responsible for a third of the global online population. At the same time, the internet has evolved into a platform where information exchange and commerce can take place rapidly and seamlessly across national borders. The internet has become a critical feature of our lives as it increases its influence on societies and economies. As a result of the internet’s ability to shape global economics and politics, the contest among geopolitical powers for setting the principles and standards of global digital governance is more intense than ever.

Since the end of the Second World War, the United States has shaped the geopolitical landscape for the better part of a century by making strategic investments in institutions of global governance. The United States transformed its foreign policy doctrine to incorporate development assistance programs and helped create the Bretton Woods institutions. Because of these early investments in the post-war period, the United States has been a critical player in ushering in a twenty-first century where the world is freer, more prosperous, and more interconnected than ever. Moreover, U.S. leadership in these institutions showcased for the world the preeminence of a democratic political system and the long-term advantages of market-oriented economic policies.

Today, digital technology is as indispensable for rapid economic development as energy, finance, and free trade. The ever-expanding scope of the internet creates competition among key democratic and non-democratic governments—notably the United States, the European Union, and China—as they seek to establish a global digital governance regime. Regulators in many countries are expanding sovereign control to push their frameworks for privacy, data protection, and digital taxation. CSIS has reported on these efforts and published its analysis on several aspects of ongoing efforts to shape this “fifth pillar” of global economic governance. In the absence of

Digital Governance
It Is Time for the United States to Lead Again

By Daniel F. Runde and Sundar R. Ramanujam

AUGUST 2021
a single international standard-setting body, the present digital governance arrangement is fragmented. However, the idea of setting up a single multilateral organization with a mandate to govern a critical economic sector is not unprecedented, with the international community having already created such institutions to regulate aviation (with the International Air Transport Association), banking (with the Bank for International Settlements), and energy (with the International Energy Agency).

The idea of setting up a single multilateral organization with a mandate to govern a critical economic sector is not unprecedented, with the international community having already created such institutions to regulate aviation (with the International Air Transport Association), banking (with the Bank for International Settlements) and energy (with the International Energy Agency).

Given the geopolitical stakes, the United States and its allies should coordinate with each other, partner with the private sector, and find common ground to create standards and to block authoritarian efforts. The following principles should form the backbone of these digital standards:

- The internet should remain free, open, and interoperable;
- National governments should ensure the free cross-border flow of data;
- Government regulations should foster innovation and the growth of emerging technologies; and
- Personal information and sensitive data should be protected from illiberal actors.

Across the world, different digital governance frameworks reflect the varied visions of the internet advocated by non-U.S. actors. Some frameworks expose the latent fault lines between close economic partners on data protection, content regulation, and competitiveness. With others, the proliferation of digital standards exacerbates trade and economic tensions. In the absence of a unified framework, competing models for digital governance have certainly raised economic costs and political tensions for the United States and its allies and competitors. Traditionally a global leader, the United States has, in recent years, retreated from the proactive role it played in international fora. The Biden administration has signaled through statements and initial actions a desire to reinvigorate multilateralism as a vehicle to achieve U.S. foreign and security policy objectives. There is also growing bipartisan support in Congress to recognize the need and the opportunity for the United States to lead in setting norms and establishing institutions for global trade and governance in digital technology. By harnessing this momentum and influencing the norms of international standard-setting institutions, the United States can secure its national interests. Further, it can catalyze global economic development by safeguarding a free, open, and interoperable internet that spurs digital innovation, meeting the needs and aspirations of the members of the international community—particularly those in emerging markets.

**CHINA’S AUTHORITARIAN VISION**

China’s desire to shape the internet’s future is most pronounced with its efforts to “reinvent” the internet in the name of regulating it. Specifically, it has led attempts...
to capture the institutions governing it and change the norms around the flow of content and data. China relies on an internet model that champions “cyber sovereignty,” where countries exercise their sovereignty over information and data exchanged online—controlling and censoring content, shutting out access in part or in whole, and enforcing data localization requirements. China receives tacit (and sometimes overt) support from other authoritarian nations, including Iran, Russia, and Saudi Arabia. Institutionally, China succeeded in winning the 2018 leadership elections for the International Telecommunication Union (ITU), a little-known UN agency whose support is needed to alter the existing internet protocol (IP) architecture—a goal that Chinese authorities have pursued for many years. Initially created to regulate the telegram industry, the ITU is now a critical stakeholder in the future regulation of the internet. The ITU operates mainly outside the public spotlight, regulating obscure technical issues like the radio frequency spectrum to more commonly noticed issues like the cost of over-the-top streaming services. If successfully implemented at the ITU, the new IP architecture (and the Chinese vision of the future of the digital sector) could lead to a fragmentation of the internet, allowing state operators to erect their firewalls and hurting the prospects for future technological innovations while undermining the civil rights and liberties of citizens. The Chinese model of digital governance is not just limited to internet standards and regulations. Chinese players in the digital economy have adopted business strategies that heavily rely on a data-extractive operational model. Consequently, as Chinese digital payment systems and other applications grow their user base, it becomes easier for the Chinese state to undermine user privacy and enhance its surveillance system.

Nearly a quarter of all internet users worldwide live in China, giving Chinese technology companies a substantial domestic market advantage. As Congress, CSIS, and other scholars have previously reported, China’s autocratic government uses this advantage to develop, test, and institutionalize digital tools that sustain its oppressive regime. China also exports some of this technology through the Digital Silk Road to undermine freedom and democratic values globally. China has been particularly successful in offering its technological prowess in 5G communications as a low-cost model to several low- and lower-middle-income countries with a growing middle class that is increasingly anxious to modernize its economy for the twenty-first century. For instance, even as Britain, India, and several European countries joined the United States in blocking Chinese 5G network firms from gaining a foothold in their markets, Huawei has been successful in building over 70 percent of Africa’s 4G infrastructure capacity and will create 5G capacity for large countries, such as South Africa. As the number of Digital Silk Road recipients continues to expand—and with the global pandemic accelerating digital transformation in many developing countries—billions of people remain vulnerable to illiberal state actions, such as surveillance, increased state control of online content and censorship, and data localization.

Should China win the race to institutionalize digital economy governance and technology standards globally, the world will see a stark decline in personal freedoms and an increase in oppression while innovation and competition suffer. Developing countries whose information and communications technology (ICT) infrastructure capacity is developed by Chinese entities will also be affected, as they become subject to autocratic standards that limit freedom and civil liberties domestically and that accelerate the painful global decline into authoritarianism. To effectively respond to China’s technological offensive, democratic societies need to coalesce and offer an alternative—first for themselves, and then to the developing world. Not unlike in the mid-1940s when the Bretton Woods institutions were set up, strategic investments in the form of financial and political capital need to be made in the multilateral system. But even before they embark on such efforts, the club of democracies will need to bridge a few critical philosophical differences on how they conceptualize digital governance.

**Should China win the race to institutionalize digital economy governance and technology standards globally, the world will see a stark decline in personal freedoms and an increase in oppression while innovation and competition suffer.**
alternative for digital governance. Seeking to respond to geopolitical forces and recognizing that the global economy is increasingly dependent on digital technologies, the European Union has adopted a user-privacy-first approach to digital governance regulations, with the most significant efforts resulting in the **General Data Protection Regulation (GDPR)**. From personal data privacy to fair competition in the markets, Brussels was among the first to forge a democratic model that sought to protect privacy and rights. The GDPR was **first passed in the European Parliament in 2014** with overwhelming consensus—approved by 621 of the 653 legislative members. However, it took another two years to **reach an agreement** between the European Council, European Parliament, and the European Commission. Countries then had two years to enact the GDPR through statutes and laws. Because of the transparent rules-based process that created the GDPR and the significant transition period for the law to come into effect, companies were able to modify their operations in the European Union and ensure compliance quickly. Further, the European Union not only had a substantial domestic market for digital products and services but also worked to promote these standards through **bilateral trade agreements**.

**Proponents of the GDPR** assert that providing consumers greater control over their data can help maintain internet freedom and openness even as large tech companies and powerful governments have increased their power to influence the internet. While the GDPR may be best known for its measures that expand personal data protection, it can also **bolster the cybersecurity efforts** of firms and prevent possible damages from data breaches and loss. Furthermore, compliance with regulation like the GDPR is a powerful way for businesses to increase consumer trust, especially when **an overwhelming majority** of U.S. citizens feel that they have little to no control over data collected.

However, **critics have argued** that while the data governance models championed by the European Union are committed to the user’s privacy and civil liberties, they are not balanced in design to support a thriving private sector, with the regulations stifling competition and dampening the spirit of innovation. For instance, the European Union created a **single data market** where public and private organizations freely pool and share their data on select sectors, arguing that such a regime would only have net **social benefits**. In effect, this kind of single data market creates an incentive structure that penalizes companies that can effectively harness data and that have invested in sophisticated systems to analyze it. Instead, it favors those in the market with less potent or outdated data systems, allowing them to benefit as “free-riders” from those who took risks and put in investments. When these rules are enforced, the European Union may burden businesses and firms with added compliance requirements that not all companies can achieve. Even a small restaurant using smart technologies for reservations collects data on customer behavior, but it does not ordinarily have the capacity to make all such data publicly available. Finally, as data helps companies develop better strategies to increase sales and boost profits, many companies develop proprietary technology to become more sophisticated with data collection and analytics. Compelling companies to make their data public flattens market competition, hurts the ability to launch innovative campaigns, and effectively creates a “stalemate.”

**EMERGING MARKETS: WHERE THE MODELS WILL COMPETE**

As their middle class grows, emerging market countries are increasingly anxious to **adopt science, technology, and innovation** to meet the burgeoning demands of their population. Emerging market countries need a model that is open in principle and viable in design. Both emerging and more developed markets would benefit from shared principles for digital governance that present clear—and beneficial—alternatives to the authoritarian and fragmented version of the internet championed by China. However, finding these shared principles will require a delicate balancing act that has long eluded policymakers. Even within the United States, **several states** have enacted (or are actively considering) legislation at the state level, like the **California Consumer Privacy Act (CCPA)**. This phenomenon is likely in response to the lack of a federal coordination framework to regulate the internet, complicating U.S. efforts to be the “standard-maker” for global digital governance.

Countries in the developing world can draw on either the Chinese model or the EU model. With the technology sector already compliant with the GDPR, firms have incentives to encourage other markets in the developing world to adopt these regulations if they have not done so already. While the perils of digital authoritarianism are clear, the impact of regulatory frameworks like the European Union’s GDPR on emerging market economies is less so. Many of these emerging market economies lack a **fully developed infrastructure** and have limited state capacities. In some cases, their free-market institutions were established within the last 20 years and can (at
best) boast a mixed record. If developing countries adopt the ELI model for internet governance, they risk various challenges. Extensive regulatory practices proposed under the GDPR will strain the state of its scarce resources with enforcement obligations, and they will tax a budding private sector with excessive compliance requirements that could hamper the ability to take initiative and innovate. One study finds that the high costs imposed on firms by the GDPR will naturally favor large multinational corporations—already in compliance in Europe and with substantial resources—over smaller, medium-sized, or indigenous alternatives, further hurting competition.

Some countries have already started to use these two models as inspirations for their own “independent” path to governing the digital economy, elevating the risks for a fragmented internet. Perhaps the most alarming is India, one of the biggest markets by userbase for several technology corporations. The Indian parliament is currently considering the Personal Data Protection Bill of 2019 to address data use and privacy concerns. If enacted into law, India will establish a Data Protection Authority at the federal level to govern private sector data usage (including processing, storage, and protection) that resembles the GDPR guidelines. However, Section 35 of the law creates pathways for getting “exemptions” from these provisions. These exemptions grant the federal political executive broad powers to access sensitive information in the “interest of security and public order,” strengthening India’s ability to conduct surveillance.

While the pending legislative action in India certainly raises concerns around the state control of personal and sensitive data, there are also less ominous attempts by national governments seeking to create their own “independent” path. Singapore was a relatively early mover in the data privacy space, with the Personal Data Protection Act (PDPA) passed in 2012 and entering into force in 2014. The PDPA covers all companies that collect personal data on Singapore residents, regardless of their physical operations. The original iteration of the law has received criticism for its failure to comprehensively protect personal data, both in its provisions and its enforcement. In response, Singapore recently passed an amendment to enhance privacy which came into effect on February 1, 2021. The amendment modifies consent provisions, increases accountability, includes data portability obligations, enhances enforcement, and more. It remains to be seen whether implementation will result in a substantial shift in Singapore’s privacy regime. However, regardless of the amendment, the PDPA diverges from the GDPR in the sense that the law does not apply to public institutions, making it an incomplete model for developing countries where sufficient safeguards on the state are not readily present.

Globally, people are concerned about how their data is used and how their online activities are regulated. A recent survey found that more than 70 percent of people are increasingly concerned about their online privacy and want regulations governing how technology firms collect and use their data. These concerns are in part a reaction to a spate of cyberattacks in the past few years which compromised sensitive personal information stored by private firms. More significantly, though, users are apprehensive of how data from their online activities is being harvested without their consent. Countries are responding to this in a piecemeal fashion without a principled approach, with some governments contemplating strong data localization laws that would curb cross-border data flows to protect “sovereign interests.” Furthermore, countries are also leaning on their political institutions to institute digital tax regimes, expand the state’s mandate to regulate digital media content, and push for other measures in the hopes of increasing competition in the technology sector. Most alarmingly, countries are successfully adopting digital tools of repression that are being exported by authoritarian regimes. Consider Myanmar, where there are reports that the military junta (after a coup d’état deposed Aung San Suu Kyi in February 2021) was using Chinese facial recognition technology to track and persecute pro-democracy protestors and institute a “digital dictatorship.”

At the same time, overly protective efforts can stifle the very spirit that built the internet into the force for economic growth that it is today, especially when done unilaterally by individual national governments. As this patchwork of national laws continues to grow, the internet’s interoperability continues to decline, while the digital economy loses its innovative edge. Moreover, the proliferation of national internet laws is also a clear indication of a leadership vacuum for digital governance in the multilateral arena.

BUILDING A COALITION FOR AN AFFIRMATIVE APPROACH TO DIGITAL GOVERNANCE

For more than three-quarters of a century, the United States has been at the helm of global leadership. Friends and foes alike have acknowledged the certain and predictable nature of U.S. foreign policy. These traits
are hallmarks of a dependable geopolitical leader and have empowered the United States to forge partnerships with like-minded nations abroad. By coupling these relationships with its leadership in multilateral institutions like the United Nations and the Bretton Woods institutions, the United States has effectively steered the international community toward prosperity, stability, and sustainable development. In doing so, it has also been able to assume the role of “standard-maker,” from the rule of law and accountable governance to economic regulations governing aviation, energy, finance, and telephony. As we undergo the fourth industrial revolution, and with China and Russia driving the global authoritarian resurgence, the United States needs to claim the mantle to deliver a universally accepted digital governance framework.

Since it became global in the early 1990s, the internet has served as a democratizing force, making it the single most consequential U.S. cultural export. Although it was never conceived with this intent, the internet today is a key instrument within the United States soft-power toolkit, as it has become a platform that facilitates political organization and dissent in the most repressed parts of the world. Any continued fragmentation of the internet owing to regressive regulatory policies and lack of U.S. action will be detrimental to U.S. interests.

As countries seek their own responses, the United States should recognize that governments are anxious to institutionalize digital regulation while risking the fragmentation of the internet. By strategically using its bilateral channels and leveraging its status as the lead shareholder in various multilateral institutions, the United States should galvanize global democracies and create consensus on digital governance principles that will protect the free, open, and interoperable nature of the internet.

To realize this arduous goal, the Biden administration should bring together two critical groups. First, the administration needs the bipartisan support of Congress as it defines its principles on digital governance, especially as it pertains to data flow, trust, privacy, and security. Although there are long-term domestic political implications to instituting federal regulations for data and content governance, it is critical that U.S. officials speak in one voice and on behalf of a diverse coalition of lawmakers, ideally both at the national and state levels. Moreover, such cross-ideological support will also ensure that the resulting regulatory framework is protected from political shifts in Washington and that it facilitates a stable U.S. policy overseas.

The second group that the United States should closely coordinate with is its transatlantic and transpacific allies. In particular, U.S. officials should engage with EU leaders to work out shared interests and commitments in tackling data governance issues. Washington and Brussels diverge on critical concepts—such as whether personal data privacy is a fundamental right, or what the scope of government Table 1: Bipartisan Legislation in the 117th Congress

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.R. 1251</td>
<td>Cyber Diplomacy Act of 2021</td>
</tr>
<tr>
<td>S. 1169</td>
<td>Strategic Competition Act of 2021</td>
</tr>
<tr>
<td>S. 1260</td>
<td>United States Innovation and Competition Act of 2021 (Passed the U.S. Senate on June 8, 2021)</td>
</tr>
<tr>
<td>H.R. 2731</td>
<td>House</td>
</tr>
<tr>
<td>S. 604</td>
<td>Democracy Technology Partnership Act</td>
</tr>
<tr>
<td>S. 224</td>
<td>Promoting Digital Privacy Technologies Act</td>
</tr>
<tr>
<td>H.R. 847</td>
<td>House</td>
</tr>
<tr>
<td>S. 687</td>
<td>STRATEGIC Act</td>
</tr>
<tr>
<td>H.R. 1816</td>
<td>Information Transparency &amp; Personal Data Control Act</td>
</tr>
<tr>
<td>S. 1353</td>
<td>Advancing American AI Act</td>
</tr>
<tr>
<td>S. 919</td>
<td>Data Care Act of 2021</td>
</tr>
</tbody>
</table>

Source: CSIS analysis.
intervention should be in promoting innovation and fair market competition. But despite these conceptual divergences, U.S. and European lawmakers are more closely aligned on the principles and values necessary to contain the rising influence from authoritarian actors in Beijing and Moscow. This brief posits a four-point strategy that can help the Biden administration not only balance its relationship between these two critical actors but also enable an alternative for the developing world that safeguards liberal democratic institutions without hampering economic growth:

- Develop domestic standards and technologies through private sector partnerships
- Engage multilateral institutions
- Promote governance standards through trade agreements with developing countries
- Facilitate capacity building and strengthening

**Figure 2: U.S. Leadership in Digital Governance**

1. **Develop Domestic Standards and Technologies through Private Sector Partnerships**

U.S. leadership in global digital governance needs to be more than a campaign of rejections. Instead, it should be supplemented through an affirmative and constructive vision that champions a viable governance model at home. Although a bipartisan legislative effort to govern the digital economy at the federal level will need deft navigation of domestic political fault lines, the United States should not let this challenge keep it from reclaiming its moral leadership and protecting one of its most influential soft-power tools. Moreover, digital governance standards developed by the United States are very likely to be steeped in common law traditions, making them less prescriptive than the European GDPR even as both seek to realize similar goals of protecting data and the digital consumer. This is a critical feature of U.S. regulatory practices that, when adopted overseas, can positively impact emerging markets.

However, the current political environment significantly limits the viability of any federal leadership on this matter. Both at the national and state levels, political actors are vastly divergent in their views on the role of the internet and the regulation of the digital economy. Congress should resolve to overcome these differences. The Biden administration can also leverage the growing bipartisan chorus of concern over China’s geopolitical influence as it works with Congress to develop domestic technological standards. A failure to act will result in the United States abdicating leadership on setting the most critical standard for the twenty-first century.

First, Congress should prioritize action on a federal privacy code for regulating data use. Like the rest of the world, people in the United States have concerns about how their data is used, and public support for expanded privacy regulations is at an all-time high. The United States has also enjoyed a long tradition of protecting privacy as an individual liberty in the healthcare and financial sectors. As scholars have noted, U.S. state lawmakers have either enacted or are strongly considering legislative actions on digital data privacy, treating them as an extension of historical attitudes toward consumer privacy. Given these factors—along with the Biden administration’s support for federal data privacy standards and the raised geopolitical stakes—Congress has before it a bipartisan and ripe opportunity for members to work together on an issue where there is a genuine cross-ideological consensus.

The administration needs the bipartisan support of Congress as it defines its principles on digital governance, especially as it pertains to data flow, trust, privacy, and security.

To that end, Congress should establish a task force that reviews existing gaps in federal laws. It should further
draft legislation that closes those gaps and harmonizes the patchwork of digital privacy policies adopted by individual states, such as California. Congress should also make significant investments into public-private partnerships to ensure that the most cutting-edge privacy-enhancing technologies (PETs) are available for public welfare. The Promoting Digital Privacy Technologies Act, legislation with broad bipartisan support in both chambers, can be of value here. If it is enacted into law, the National Science Foundation will be authorized to work with the private sector to promote and invest in research developing PETs. Additionally, the law would require the National Institute of Standards and Technology to work with public and private sector actors to create “voluntary consensus standards” that would incorporate PETs into various data-collection and usage applications.

Finally, Congress should put the United States in the international driver’s seat such that it takes the lead in the regulation of artificial intelligence (AI). Building on past CSIS reporting, this brief recognizes that preserving the U.S. innovative edge in critical frontier technologies is relevant to geopolitical competition with China, and that global attitudes toward AI regulation will impact innovation. The 116th Congress failed to pass a bipartisan resolution that laid out AI regulation principles comprehensively and demonstrated a market-and-innovation-friendly approach to protect U.S. national security equities while addressing the risks of AI to democratic values. By reconsidering those measures, the United States can shape the global AI governance framework, preserve AI’s potential to flourish, and catalyze economic development without exacerbating the global digital divide.

2. **Engage Multilateral Institutions**

As domestic regulatory frameworks and standards are developed, the United States should engage with multilateral actors to promote them and the values that exist at their core. Debates on global digital governance are ongoing in various multilateral platforms. Achieving a universal agreement on digital governance standards is not an easy—or even a realistic—goal, especially considering that even like-minded partners in Brussels and Washington disagree on critical concepts like privacy and consumer protection. Nevertheless, U.S. officials should be open to compromise as they pursue diplomatic efforts using a domestic governance framework, with the objective of finding consensus with market democracies that can protect a free, open, and interoperable internet.

The Biden administration has time and again signaled its eagerness to restore the prominence of multilateralism in its foreign policy doctrine. In a recent Washington Post column, President Biden reiterated this commitment ahead of his participation at the 47th G7 summit and emphasized the need for the world’s market democracies to come together to ensure that it is their values—not those of autocrats—that govern the use and development of new technologies. The Biden administration will have to realize these commitments through meticulous diplomatic lobbying, by bringing together partners and allies and harnessing the momentum built by powerful country clubs (like the G7 and G20) and regional blocs (like the Asia-Pacific Economic Cooperation) on harmonizing digital governance standards. The Carbis Bay G7 Summit gave the leaders an opportunity to emphatically reaffirm their commitment to protecting global institutions as a means of preserving and promoting democratic values. Relatedly, the leaders also made clear their commitment to collaborate on shaping digital technical standards. The Biden administration should build on this momentum among democratic societies to push for a shared concept of digital governance at the Rome G20 Summit in the fall. As the 20 largest economies of the world convene in Italy, the United States should lead the democratic alliance to build on the 2019 Osaka Declaration on Digital Economy and operationalize the G20 communiqué that expressed the club’s commitment toward a free, open, and interoperable internet by ensuring the free cross-border flow of data while preserving privacy and security. In addition, as the administration plans to convene a “Global Democracy Summit,” it should consider using this coalition of democracies to exclusively develop harmonized policy frameworks that combat the growing pains of digital authoritarianism. Leaders of allied nations and senior members of the administration have also expressed their desire for a new democratic group of nations called the D10 (indicating that Australia, India, and South Korea should be added to the club of G7 democracies).

Building consensus through informal and loosely held coalitions is only part of the U.S. multilateral engagement strategy. This consensus is a critical prerequisite for the United States’ efforts to reorient
multilateral institutions into standard-setting bodies that promote governance models that are rooted in democratic values and are resilient to authoritarian excesses. A key organization in the global standard-setting game is the previously referenced ITU. The ITU comprises 193 nation-states and 900 non-state sector members (including private sector organizations and civil society actors), reflecting the technical nature of an organization that can fundamentally alter the multistakeholder and interoperable internet model. The incumbent secretary-general, Zhao Houlin, will vacate his office by 2022, and his successor will need to be chosen. Already, the State Department has announced its support for a U.S. candidate—Doreen Bogdan-Martin—for the organization’s top job. But beyond this announcement of support, the Biden administration needs to allocate significant time, resources, and effort to ensure that Bogdan-Martin wins the contest. With the only other official candidate being Russia’s Rashid Ismailov (a former Huawei executive), Bogdan-Martin’s loss would mean that market democracies will take the back seat as Russia (and other authoritarians) continue their influence in the organization until 2026. With the United States emerging successful in ensuring the victory of its preferred candidate—Daren Tang of Singapore—in the World Intellectual Property Organization elections (also an essential organization for global digital security), the United States should channel the consensus it has built with its democratic allies to determine a viable pathway for electoral victory in the ITU, both for the secretary-general position and for down-ballot races.

3. Promote Governance Standards through Trade Agreements with Developing Countries

As it builds consensus among the leading market democracies, the United States should also proactively engage with developing countries on digital governance, especially on issues of privacy and cross-border data flows. Free trade agreements are instrumental here, as they can serve as a platform for the United States to promote its standards on data protection and privacy regulations among emerging market economies.

This strategy’s “gold standard” lies in the digital trade chapter within the U.S.-Mexico-Canada Agreement (USMCA). Heavily inspired by the erstwhile Trans-Pacific Partnership agreement, USMCA’s digital trade chapter marked the first time in the history of U.S. trade policy that a broad range of digital governance issues was covered so comprehensively. Moreover, with the signing and ratification of the USMCA, the signatories were bound by a legal agreement that banned them from adopting data localization policies while obligating each country to establish its own personal information protection laws to address privacy concerns.

The United States should seek to replicate and scale up the USMCA model with developing countries. Such a move would coincide with the efforts already taken by Britain, Japan, and the European Union, all of whom have sought to use trade agreements as a vehicle to promote their values and principles of digital governance. The United States and the European Union have also made progress bilaterally with the establishment of the high-level EU-U.S. Trade and Technology Council that seeks to address and eliminate technical barriers while growing partnerships around technology and digital issues between Washington and Brussels. Though painstakingly slow and politically strenuous, trade agreements are sustainable and legally enforceable in the near term.

Proactively promoting U.S. digital principles through trade agreements will allow the United States to reach developing countries and give them the option to adopt (or refuse) a digital governance model that restrains illiberalism and addresses an increasingly anxious population’s privacy concerns without stretching thin the already limited state capacity. More importantly, this will not create impediments for countries with budding indigenous emerging technologies that need free and flexible access to data. As CSIS has previously argued, the Biden administration can also explore the use of non-binding data governance principles (depending on the country context) to experiment with cross-border data flow regulations, with the ultimate aim of securing international consensus on data governance. In the long run, these efforts will be integral to U.S. leadership in digital governance, as they increasingly grow the number of countries aligning themselves to U.S. digital governance standards—effectively lowering the threshold for the world to adopt the U.S. model as the prevailing one.

4. Facilitate Capacity Building and Strengthening

U.S. leadership in the area will remain incomplete if developing countries remain under-equipped or
ill-trained to implement the prevailing governance model in their domestic contexts. Fortunately, various U.S. federal agencies have had a history of engaging in country-level partnerships to train public officials overseas in the best practices for implementation. The spirit of this engagement can be captured by the recent signing of a letter of intent between the U.S. Agency for International Development (USAID) and ITU, agreeing to strengthen collaboration so as “to promote open, interoperable, and secure ICT infrastructure in developing countries.”

Consistent with this spirit, U.S. officials should consider using the digital development principles as a foundation for ensuring that new digital efforts are responsive to long-standing development values. The development community will also need to mainstream digital standards into all its sectors, and it will need to train staff that work on a range of portfolios—from democracy promotion to energy—to understand the impact of digitization.

U.S. officials should also expand upon the Digital Ecosystem Assessments (DECAs) it piloted in 2019, which have now been completed for Kenya and Colombia. These reports allow development practitioners to build on a strong understanding of the current need and context and to create programming that is context driven. Depending on what they learn from the DECAs, development practitioners will need to adopt programming mechanisms to advance the digital development agenda. Furthermore, the Digital Connectivity and Cybersecurity Partnership between USAID and the U.S. Department of State is a critical mechanism that can improve local capacity and regulatory systems. To ensure its success, it is important that Congress and the Biden administration sustain it with additional resources. In part, this can be achieved by effectively using the USAID Digital Ecosystem Fund (DEF) and bolstering it with additional funding to help train and equip policymakers overseas in digital governance.

Finally, the FY20 Countering Chinese Influence Fund (CCIF) specifically calls out digital norm-setting and regulation. Providing these mechanisms with additional CCIF resources will show a strong commitment to a favorable alternative to Chinese actions in the digital sphere.

Daniel F. Runde is senior vice president, director of the Project on Prosperity and Development, and holds the William A. Schreyer Chair in Global Analysis at the Center for Strategic and International Studies (CSIS) in Washington, D.C.

Sundar R. Ramanujam is a research associate with the CSIS Project on Prosperity and Development.

The authors would like to thank Christine Li for the invaluable research efforts critical to producing this brief.

Support for this publication was provided by Google. The views expressed here do not necessarily reflect the views of Google.