AMERICAN LEADERSHIP INITIATIVE

A Global Digital Strategy For America

A Roadmap to Build Back a More Inclusive Economy, Protect Democracy and Meet the China Challenge

February 2021

Table of Contents

Introduction & Summary

The digital revolution is permeating all aspects of society, remaking the way people work and learn, changing the economic landscape, and altering America's relationships with the rest of the world. While this revolution has generated many benefits throughout society, the rapid change, accelerated by the global COVID-19 pandemic, has also created economic disruption, devastating many in the middle and working classes and posing challenges to American democracy. With the right policies, however, this revolution holds the potential to create a more inclusive and growing American economy with good American jobs, establish digital governance to protect democracy, support inclusive growth in developing countries, and position the United States (U.S.) as a global digital leader.

That is why the American Leadership Initiative (ALI) has convened and consulted with experts and key stakeholders from think tanks, academia, civil society, and business, together with elected officials, to develop a digital policy roadmap for the Biden Administration and Congress. This report represents a culmination of that work.

To reap the benefits of the digital economy, and avoid its pitfalls, America must launch a **Global Digital Strategy,** involving a whole of government approach, and including participation of business and labor representatives, and civil society stakeholders. Such a strategy should focus on two interrelated pillars: **Investing in America,** ensuring equal access to technology to close the digital divide and promoting policies to ensure American competitiveness; and **Leading Globally,** working with allies to create a global digital future that is open, transparent, and democratic.

America's global digital leadership requires citizens who have equal access to broadband, digital technologies, training, and education, so that they can fill the jobs of today and tomorrow, actions made more urgent by the unequal social and economic impacts of the pandemic. **Investing in America** must therefore start with a comprehensive look at how to

improve access to digital training at all levels, from grade school through community college and apprenticeships, to older workers who need to upskill for new jobs. It must include providing access to digital devices and broadband for all citizens and ensure that this training and technology is accessible to citizens living in rural America, African Americans, Hispanics, and other underserved communities.

To ensure American workers are gaining the right digital skills necessary to succeed in the future economy, government, corporate and labor partners must come to the table to significantly bolster education and training programs in new ways. By developing an inclusive digital agenda, including universal access to broadband, as well as freeing up new spectrum and tackling net neutrality, the new Administration can shift the U.S. economy towards greater income equality and prepare American workers to compete globally in an increasingly digital world.

The Biden Administration should also move to establish an Office of Global Digital Policy in the Executive Office of the President. This new office would coordinate digital policies, starting with the imperative of doubling U.S. federal investment in research and development; advancing a global digital governance agenda that allows citizens to safely use the internet; identifying a limited group of technologies for targeted support; encouraging policies that foster innovation, protect key technologies, promote exports; and supporting immigration reform, including provisions designed to attract and keep the best talent from abroad.

These efforts must be combined with a multipronged series of investment and export controls to protect key U.S. technologies and a Digital Marshall Plan to provide financing for U.S. technology companies. This financing would allow companies to compete on a level playing field with China's technology companies that receive government subsidized financing, not just to provide fair commercial competition, but to ensure that developing countries can purchase internet infrastructure consistent with an open, accountable, and democratic internet, as opposed to Chinese supplied

infrastructure, which supports an autocratic internet, allowing government monitoring and censorship.

With strong, inclusive domestic policies and funding, America and its workers will be positioned to compete and **Lead Globally**. To achieve such global leadership, the Biden Administration must discard the unilateral approach of the Trump Administration and establish an alliance with other liberal democracies that have advanced technology industries. These technology-driven democracies, the "T-10," should work together to create a global governance agenda, based on shared values. This alliance should create a framework that will allow businesses, civil society, and citizens access to an internet that is open, democratic, and safe, as well as form a template for negotiating digital agreements with other countries, understanding that other countries may need to phase in or adapt parts of the agenda.

Finally, the U.S. must work with its allies to develop a coordinated approach to China, applying joint pressure to eliminate the subsidies and other non-market practices it uses to give its technology companies an unfair advantage, while jointly coordinating the protection of technologies vital to national security. This leadership will be important in safeguarding American interests and a democratic internet, especially when faced with a rising China, which is promoting an autocratic internet as an export and political strategy.

With the T-10 framework in place, the U.S. should negotiate additional digital arrangements. The next step should be the negotiation of a Pacific Digital Agreement, taking advantage of the digital agreements many of these countries have already negotiated among themselves. This agreement would also be a way for the U.S. to reassert its engagement in Asia, a region that has sorely felt the U.S. absence during the past four years.

A comprehensive digital strategy is broad and complex, touching on almost every aspect of the economy and people's lives. New technologies offer the promise of solving many of the world's challenges but also raise

new issues, like increasing economic inequality, managing the impact of violent and false narratives on social media, and the opportunity to abuse technologies like facial recognition. Our list of recommendations detailed in this report is not exhaustive, but rather provides a policy scaffolding – the key elements that must be in place for the U.S. to harness digital technologies to their best advantage, creating a more inclusive and growing economy at home and abroad, and a safer, more democratic world.

About the American Leadership Initiative

The American Leadership Initiative (ALI) is working with elected officials and other stakeholders to develop a 21st century vision and policy agenda for American global leadership, based on American interests and shared values. ALI's policy work is focused on five pillars: advancing inclusive and sustainable growth at home and abroad, pursuing smart trade policies, leading on climate, meeting the China challenge, and promoting democracy, human rights, and rule of law.

About the Authors

Dr. Orit Frenkel

Dr. Orit Frenkel is the CEO and co-founder of the American Leadership Initiative. She has 39 years of experience working on Asia, trade, and foreign policy issues. Prior to founding ALI, Orit was a senior executive with General Electric Company for 26 years. In that position, she supported GE's international public policy initiatives, international sales, and corporate social responsibility initiatives. This included addressing the policy and business challenges posed by China, developing rules for digital trade, and policies to support sales of environmentally friendly goods.

Dr. Frenkel started her career in the Office of the U.S. Trade Representative where she was the Director for Trade in High Technology Products and Deputy Director for Trade with Japan, and spent a year working for Congressman Lee Hamilton during his time as Chair of the House Foreign Affairs Committee.

She is the author of numerous published articles on trade and foreign policy issues, as well as a book on the negotiation of the U.S.-Israel Free Trade Area. She is an Adjunct Fellow with the Center on Strategic and International Studies, a member of APCO's International Advisory Committee, and has served on the board of numerous trade associations and on Department of Commerce and State Advisory panels.

Ms. Frenkel received a Ph.D.in International Economics from The Johns Hopkins University, an M.P.P. from the University of Michigan, and a B.A. in Economics with honors from University of Maryland.

Rebecca Karnak

Ms. Rebecca Karnak is Director of Digital Projects at the American Leadership Initiative. She is also the Principal and Founder of Woodside Policy LLC, a boutique public policy consulting firm. Prior to joining ALI, Ms. Karnak was Senior Director, Global Public Policy, at Dell Technologies, focused on helping the company navigate geopolitical uncertainty and build relationships and platforms to enable constructive public policy conversations.

She has held roles in government, trade associations, and non-profit settings for over two decades, including at the U.S. Department of Commerce, the U.S. Embassy in Beijing, and the Information Technology Industry Council. Ms. Karnak earned her B.A. from the Ohio State University, and her M.A. in international affairs, with language proficiency certification in Mandarin and Spanish, from the Johns Hopkins School of Advanced International Studies (SAIS).

Acknowledgements

The American Leadership Initiative consulted with a diverse group of experts and stakeholders in the preparation of this report and is grateful to the many individuals who were generous with their time and thoughts. ALI is especially grateful to the members of its Global Digital Strategy Working Group for their contributions: Edward Alden; Ed Britan; Michael Castellano; Wendy Cutler; Rebecca Fraser; Matthew Goodman; Josh Kallmer; Nicole

Lamb-Hale; Debra Marks; Josh Meltzer; David Ohrenstein; Matthew Reisman; Meredith Sumpter; Scott Thompson; Paul Triolo; Astri Van Dyke; and Debra Waggoner. Special thanks also to Claude Fontheim for his contributions. These individuals have contributed in their individual, not institutional, capacities, and support the general policy direction reflected in this roadmap, though they may not necessarily agree with every finding and recommendation.

Part I: Investing in America

Now is the time for a landmark investment in America's digital competitiveness to prepare the country for an increasingly digital post-pandemic economy. Such an effort should include investments in digital training and connectivity, the development of a digital governance regime and measures to upgrade America's technological competitiveness.

This must start at home with investments in digital education, training, and connectivity. These investments must come with implementation of diversity, equity, and inclusion policies to ensure that the benefits are widely shared among American workers without a college degree, women, Hispanics, African Americans, and indigenous Americans. This initiative would be a pivotal step toward closing income inequality in the U.S. and ensuring that all Americans have access to high-quality, good-paying jobs. Creating an inclusive and skilled workforce would strengthen American businesses, their employees, and ultimately, America's economic competitiveness.

The U.S. must also develop a comprehensive digital governance agenda that updates its policy approach to the digital economy. This digital governance agenda should embrace innovation and the potential economic and social benefits of new technology for all sectors, businesses of all sizes, and underrepresented voices, while seeking to protect consumers and citizens. It should also codify the American vision of an internet that is open, transparent, and democratic, as opposed to China's vision, which is one of censorship, monitoring and autocracy.

To promote U.S. technological competitiveness, particularly with respect to China, the U.S. should seek to reenergize U.S. competitiveness policy, including pieces that have shown dividends in the past: funding and incentives for research and development (R&D); identifying and protecting key technologies; implementing an immigration policy that attracts the best global talent;

new regulations to protect America's key technologies; and a Digital Marshall Plan to allow American firms to compete with China around the world and promote its democratic vision of technology.

A landmark investment in America's workers, its digital governance and technological competitiveness will lay the groundwork for a thriving domestic economy and position the U.S. to be a 21st century global digital leader.

Promoting Access and Inclusion

Throughout the Covid-19 pandemic, Americans have experienced more than ever how vital fast internet connections, digital devices and related skills are to daily life. Overnight, students turned to online learning, workers shifted to online work, and doctors offered telemedicine appointments, with several people in a household often using internet service at the same time. However, this online existence was not available to everyone, as 40 million people in the U.S. realized that they had unreliable internet service, or none at all.[1]

A deep digital divide that drives economic inequality is undermining American economic competitiveness. This divide also disadvantages many American workers based upon race, geography, and level of education. As of 2019, Pew Research Center[2] reported that roughly three-in-ten adults with household incomes below $30,000 a year do not own a smartphone. And more than four-in-ten don't have home broadband services or a computer. This reality increases U.S. economic inequality, leaving the U.S. unable to harness the full potential of its human capital, and weakening U.S. global competitiveness.

The continued digitization of many jobs hits low-skill workers and workers from marginalized communities especially hard, with an increasing number of traditional low-skill jobs now requiring digital skills. This trend will only accelerate over the coming years. Manufacturing workers and farmers need digital skills to operate computer-aided machines and farm equipment. Workers with a high school degree need digital skills to find work and earn a living wage. A recent Brookings Institution study concluded that acquiring digital skills

is now a prerequisite for economic success for American workers.[3] Covid-19 has accelerated this trend and upskilling the population will be an essential component to recovery for the U.S. economy.

> **Access to affordable broadband and connected devices must be a national priority.**

Access to affordable broadband, connected devices, digital training, and education for Americans must be a national priority, akin to the way the federal government prioritized the interstate highway system in the 1950s. This effort will require greater involvement and investment by business across the country and will only produce the desired outcomes if strong diversity, equity, and inclusion (DE&I) measures are implemented.

The following section regarding "access and inclusion" explores and offers recommendations to help close the digital divide by addressing several key areas: education and training, including apprenticeships and community college; access to equipment; spectrum allocation; and net neutrality, all of which need to be reprioritized and expanded as part of a package to invest in America. These changes will help ensure a much more inclusive economy and ensure that the U.S. has a workforce trained for the jobs of tomorrow and prepared to compete globally.

Education & Training

America's economic strength relies on the education and skills of its labor force. Digitization of the workplace has been transformational — two-thirds of the 13 million U.S. jobs created in the past decade required medium or advanced levels of digital skills,[4] while only 30 percent of jobs required no digital skills at all.[5] Low- and middle-skill jobs are increasingly automated, threatening to displace as much as one-third of the workforce during the next decade, widening income inequality and deepening racial and regional divides. U.S. efforts to help displaced workers in transition have been inadequate. Unemployment insurance is too rigid and covers too few workers, and training programs are often unsuccessful at matching training to available jobs.

Meanwhile, foreign competitors are doing far more than the U.S. to prepare their workforces for the future. Denmark is a world leader in adjustment supports for unemployed and displaced workers.[6] Singapore has created new lifelong learning benefits[7] so its workers can continuously upskill. Germany boasts a much-heralded apprenticeship system[8] in which 60 percent of youth train as apprentices in fields such as advanced manufacturing and IT, compared to just 5 percent in the U.S. Estonia has prioritized digital skills[9] for its citizens from early on, ensuring that all schools have Wi-Fi, computers and digital training. Today, Estonia has the smallest performance gap[10] out of Organization for Economic Co-operation and Development (OECD) countries between low- and high-income students.

By contrast, the U.S. ranks near the bottom among OECD countries on public spending on labor market programs as a share of GDP; and the trendline is headed in the wrong direction.[11]

During the past 15 years, the Department of Labor's (DOL) budget for grants to states to support job training programs has fallen by more than half after counting for inflation. Worse, the past several decades have seen steady declines in private sector investment in workforce training – with a falling share of workers receiving on-the-job or employer-sponsored training.[12]

It is critical that opportunities be dramatically expanded for citizens to acquire the digital skills they need not only for jobs today, but for the jobs of the future. This is especially true for low-skilled workers, workers without a college education, workers of color and workers from other marginalized groups. As Covid-19 has shown, the first step in building digital skills is making sure the entire country has access to broadband. K-12 students must also have access to basic digital tools and computer classes to ensure that all students finish high school with the skills needed for good jobs, an essential step to reduce the glaring inequalities in American society. It is also critical that separate funding be available to ensure that STEM education is offered in K-12 schools serving historically disadvantaged groups.

Investing in digital training for workers who are currently unemployed or

in low-wage jobs and seeking to increase their skills is equally important. Before the pandemic, 6 to 7 million jobs were unfilled in the U.S., primarily because of a mismatch between worker skills and available jobs.[13] A lack of digital skills is a major reason for this gap.[14]

In addition to repairing the inequalities in U.S. society and the economy, having a digitally-skilled population is also vital to ensuring that American business continues to have the talented labor force it needs to remain a global leader. A successful workforce model for the 21st century will require employers to think about how to develop the pipeline of talent needed to build their workforce.[15] Corporations must partner with the government to upgrade and expand digital training and education systems to ensure that workers are gaining skills that will lead not only to existing jobs, but those in years to come. Microsoft launched a program in 2020 to help 25 million people globally acquire digital skills, and Qualcomm has a program to provide STEM education in classrooms across the U.S. While some companies have initiated programs, much more needs to be done. There needs to be a much more extensive and systemic approach to facilitate public-private partnerships, ensuring that digital training is available across all U.S. population groups and education levels.

Community College

Community colleges enrolled more than 5.7 million students in 2019.[16] They play a particularly important role for students who need additional skills to find new or better paying jobs. In 2015, President Obama proposed legislation to make 2 years of community college free.[17] While the legislation did not pass, a number of states have enacted programs to make community colleges free, especially for low-income families.

Funding should be expanded for Minority Serving Institutions (MSIs) and Historically Black Colleges and Universities (HBCUs), especially for their STEM and computer science programs, to ensure that the next generation's workforce harnesses the full potential of America's citizens. In addition to making community colleges accessible, community colleges must greatly expand their digital and technical skills training to meet the growing demand

for these skills in the workplace. These programs should be created in partnership with companies that can help design courses and training that could lead to jobs in those companies. Companies should also receive incentives to partner with community colleges in developing digital job preparedness programs. Google recently initiated its first federally registered apprenticeship program with the Borough of Manhattan Community College (BMCC), San Jose City College (SJCC) and the Austin Community College District (ACC) to train IT workers. Federal incentives are needed to encourage companies to greatly expand such programs.

Enacting federal legislation to make community college more affordable for low-income families on a national level and encourage creative partnerships with industry is critical. Such legislation should specify funding for digital training and create incentives for digital companies to partner with community colleges on that training.

Apprenticeships

Historically, the U.S. has not significantly supported apprenticeship programs. Unlike workforce training, apprenticeships are closely tied to the private sector. Programs are created when and where employers see a need, typically teaching job-ready skills that frequently lead to a long-term position with a given employer. Apprenticeships are an important tool to prepare students and workers for an increasingly digitized and automated economy and can be designed for students coming out of college, community college or high school. Apprenticeships can also narrow the post-secondary achievement gaps in both gender and race.[18] Having learning take place mostly on the job, and providing participants with wages while they learn, is especially beneficial to students from low-income communities.

Demand is growing for apprenticeship programs in the U.S. In South Carolina, the state created "Apprenticeship Carolina" in 2007, in response to the business community's call for a more highly skilled labor force. There are more than 34,000 apprentices in the state today.[19]

Other countries have long made use of apprenticeship programs with im-

pressive results. Apprenticeships are a key pathway to employment for young people in Germany, whether they are pursuing a blue- or white-collar profession, with 53 percent of young people starting their careers through apprenticeships. Companies consider training a social task and take pride in being a training-focused company. The government funds the development, implementation and promotion of apprenticeships, and partners with local governments to fund sectoral and vocational training systems that supplement the apprenticeship system.[20] The Swiss apprenticeship program operates similarly and is regularly rated the best in the world. Two-thirds of Swiss students enter apprenticeship training instead of 10th grade, where they spend three-to-four days in a job setting and one-to-two days in an academic setting. These programs last three to four years, with students a part of the workforce, alongside skilled adults, earning a paycheck.[21]

In the U.S., the role of the federal government in supporting apprenticeships has largely been registering individual programs that comply with federal standards ("Registered Apprenticeships").[22] The U.S. enacted Registered Apprenticeships 80 years ago under the National Apprenticeship Act, also known as the Fitzgerald Act, which required employers to meet certain labor standards and established regulations for their programs to be recognized by the U.S. Department of Labor (DOL) and culminate in a nationally recognized credential, issued by the DOL.[23]

During the Obama Administration, there was a push to expand apprenticeship programs, including in new industries and for women and people of color.[24] Recent data show that these efforts have begun to pay off,[25] with U.S. apprenticeships growing from roughly 375,000 in 2013 to 633,000 in 2019,[26] yet still comprising only 0.3 percent of the total workforce. Historically, apprenticeships in the U.S. have been focused on manufacturing or trades, and accessed by mostly white men.[27] It should be a national priority to focus apprenticeships on digital skills and make these programs more accessible to women, Hispanics, African-Americans, and other marginalized communities. This effort can be done, in part, by partnering with MSIs, HBCUs, and similar institutions.

National apprenticeship programs must be expanded in close consultation with employers. For the private sector, investing in apprenticeship programs provides an important opportunity to develop a pipeline of skilled labor. Such cooperation also ensures that workers are trained in digital skills that will be valuable for years to come. Incentives should be provided for companies to develop apprenticeship programs, and companies must take a leadership role in building out apprenticeships.

IBM started its digital apprenticeship program in 2017, where applicants need to have a high-school diploma or GED, and has hired about 500 apprentices so far, with plans for more.[28] While this is program is a good start, the U.S. needs many times this number of apprenticeships to start to address its current and future needs.

In a positive development, the National Apprenticeship Act, which would allocate $3.5 billion over the next five years to create 1 million new apprenticeship opportunities, passed the House of Representatives in December 2020.[29] Importantly, apprenticeship programs should be updated to ensure that American workers are trained for digital occupations and available jobs requiring digital skills – ranging from basic spreadsheet and word processing skills to more advanced programming or manufacturing. Private sector demands for digital skills training will only grow, as more and more companies in all sectors become "digital companies." These apprenticeships should be available not just to young entrants to the job market, but also to older workers who will need new skills to retain or find good jobs. These programs must also expand the participation of women and minorities who are traditionally under-represented in apprenticeship programs.

Access to Equipment and Broadband

The second important component of maintaining America's digital leadership and creating a digitally prepared workforce is upgrading America's digital infrastructure and increasing access to equipment. Access to the internet is no longer a luxury, but an essential element to participate in the economy – as vital as access to electricity was a century ago. Even before the pandem-

ic, U.S. internet infrastructure lagged that of other developed countries. Last year, the U.S. ranked 10th in terms of internet connection speed, behind the Nordic countries, Japan, Hong Kong and South Korea, and 30th in terms of mobile download speed.[30]

This lag in service is even more pronounced in low-income and rural America. According to a 2019 Pew Research Center survey, only 63 percent of rural Americans said they had broadband internet connection at home, as opposed to 91 percent and 94 percent for urban and suburban families, respectively.[31] Thirty-five percent of farmers say they don't have enough connectivity to run their farm equipment.[32] As recently as 2019, 29 percent of adults with household incomes below $30,000 a year didn't own a smartphone, 44 percent didn't have home broadband services, and 46 percent didn't have a computer.[33] This gap impacts about 3 million American children (18 percent) who don't have broadband home service to do their homework.[34] Gaps in access to equipment and internet are especially stark for low-income Americans, a divide that hits Hispanic Americans and African Americans hard. One-third 0f African Americans and Hispanics — 14 million and 17 million, respectively — still don't have access to computers or tablets in their homes, and 35 percent of African American households and 29 percent of Hispanic households, do not have broadband.[35]

In January 2020, the Federal Communications Commission (FCC) launched the Rural Digital Opportunity Fund which would allocate $20.4 billion over 10 years to expand rural broadband.[36] However, FCC and industry experts estimate it will cost up to $80 billion to achieve universal broadband connection in the U.S.[37] To address this need, the Center for Rural Innovation suggests creating a new federal loan program that would offer 50-year no-interest loans to communities and co-ops so rural public-private coalitions can build broadband networks.[38]

There have been several bills introduced in Congress to expand broadband and accelerate deployment of the FCC 5G Fund for Rural America.[39] For example, Representative James Clyburn and Senator Amy Klobuchar both introduced legislation this summer that includes $80 billion for the deployment

of nationwide high-speed broadband, funding for no-interest loans to communities as well as funding to subsidize internet usage for low-income households.[40]

> **Investment in rural broadband must support installation of the latest 5G technology.**

Investment in rural broadband must support installation of the latest 5G technology. Proposals have been advanced to put in older technology in rural areas, which would be less expensive, however, such an approach would leave these communities continually at a technological disadvantage to the rest of the country. When an investment is made, it should be in the newest technology to ensure technological parity for all communities. Given the urgent need, it is critical that the funding not be tied to administratively burdensome rules making it difficult to distribute, and funding should be targeted to those opportunities that allow for the rapid deployment of broadband. Congress must also provide funding to enable the FCC to establish accurate maps to identify where 5G is needed.

In addition to making the internet more accessible to rural and low-income Americans, programs should be established to subsidize computers, tablets, and smartphones for those below certain income thresholds. Each of these technologies is nearly ubiquitous among adults in households earning $100,000 or more a year, with most upper-income households owning multiple devices. For those without devices, it means difficulty in accomplishing tasks that have become a necessity during Covid-19, like doing homework or accessing telemedicine appointments.

Investments should also be made to upgrade America's overall broadband system. The pandemic has seen a dramatic acceleration in internet usage, driving almost a year's worth of traffic growth in the span of a couple of weeks.[41] This crisis has launched a paradigm shift in which millions of Americans have incorporated the internet as a critical part of their personal and professional lives. This will not change after the pandemic. This shift necessitates an upgrade to the national broadband system to allow for increased speed and traffic, whether through accelerating the move toward 5G, Open Ran, or other technologies.

Spectrum

Spectrum is a finite resource. Roughly 60 percent of spectrum bands are under government control and freeing up new spectrum can take more than a decade. To meet consumer demand and lead the world in 5G and innovation, wireless networks need hundreds of megahertz of new spectrum, especially the mid- and high-band spectrum, which 5G uses.

Several strategies are available to free up new spectrum. The first involves the FCC identifying where currently allocated spectrum is overly generous as compared to usage. This requires in-depth conversations with numerous stakeholders, including the public. Secondly, there are areas where spectrum may have been allocated on the premise of a future technology which never developed. Spectrum sharing, where the National Telecommunications and Information Administration (NTIA) works with the FCC and federal agencies to make spectrum available for wireless service providers to meet the ever-increasing demand for advanced services, while ensuring federal agencies have access to the spectrum to perform critical missions, is another means to free up spectrum that has seen some success.[42] Finally, the Department of Defense (DOD) holds a significant amount of spectrum for national security purposes, some of which could be released for commercial use.

In sum, Congress, the FCC, and NTIA need to work together to free up additional spectrum for wireless use.[43] Policymakers have recently taken steps to unlock key spectrum opportunities, but that work needs to be accelerated to deliver a dedicated spectrum pipeline in the near-term.[44]

Net Neutrality

Net neutrality refers to the concept that, notwithstanding reasonable network management practices, internet service providers (ISPs) should treat internet traffic equally, regardless of its kind, source, or destination.

Little regulation existed to ensure these protections in the U.S. before 2010, while other countries moved forward with rules intended to balance the interests of both ISPs and users.[45]

In the early 2000s, consumer complaints arose due to service providers prioritizing certain content flowing through their cables and cell towers and blocking or slowing other content. Telecom companies can block or slow access to a service like Skype, or slow down Netflix or Hulu, to steer consumers to keep their cable package or buy a different video-streaming service from which the service provider would benefit. For example, in one of the first efforts to enforce early net neutrality rules in 2005, North Carolina ISP Madison River blocked Vonage, a service for making telephone calls over the internet. The FCC fined Madison River and ordered it to stop blocking.[46]

Civil society groups have argued that the lack of net neutrality disadvantages lower income consumers, who may be offered slower speed services. Telecom companies have asserted that net neutrality regulations will stall the development of new internet technologies and hamper efforts to separate data that is more essential and mission critical; for example, data transmitted between autonomous cars or medical devices.

In 2015, the FCC issued a sweeping net neutrality order that changed the classification of internet service from an "information" to a "common carrier" service. The internet had originally been classified as a "Title I information service" or a Title I service under FCC rules. This meant that the service and its service providers would be left largely unrestricted by the FCC, in contrast with a "Title II common carrier service," which is more strictly regulated. The difference between the two services has been characterized as the difference between a luxury, like cable television, and protected and ensured telephone service.[47]

In 2017, those rules were revoked, and new FCC rules eliminated the common-carrier status for service providers, along with restrictions on blocking or slowing content. Instead, the new rules require that providers disclose information about their network-management practices.

While Congress has been unsuccessful in its attempts to pass legislation restoring the internet's Title I status or otherwise supporting net neutrality, several U.S. states have passed legislation to make net neutrality a require-

ment. Washington became the first in March 2018, and Oregon followed soon after.[48] California passed one of the most comprehensive net neutrality laws of all, but the rules are currently on hold amid a legal challenge from the federal government.[49]

The European Union, in contrast, approved rules in 2015 requiring service providers to handle internet traffic equally, leaving flexibility to restrict traffic when network equipment was operating at its maximum capacity. The rules also allow traffic restrictions to protect network security and handle emergency situations.

Some have argued that the net neutrality debate should consider the Internet of Things (IoT), which is already increasing its share of internet traffic, beyond discussion of video streaming and other applications.[50] In a letter to the FCC, officials in New York, San Francisco, Portland, and other U.S. cities said that giving control of the internet to ISPs through the reversal of 2015 net neutrality rules would affect smart city projects, making it costlier and more difficult for city governments to deploy IoT technologies related to safety and smart street lights.[51]

The U.S. has long been a leader in developing policies that balance free speech and consumer protection with opportunities for research and business innovation. Congress should return to the question of creating balanced legislation on net neutrality that provides equal access to all consumers, while creating incentives for businesses to provide internet access for all.

Adopting a Digital Governance Agenda

The U.S. has long led in technology innovation, and U.S. tech companies are key drivers of economic growth and competitiveness. American digital services exports are now $517 billion per year, generating a U.S. digital trade surplus of $220 billion. U.S. companies rank high in global market share for artificial intelligence, hardware, e-commerce, digital advertising, operating

systems, the app economy, cloud technologies, social media, the sharing economy, data analytics, and other innovative internet technologies. Finally, digital services are helping U.S. small businesses overcome new challenges during the Covid-19 pandemic. One in three small- and medium-sized businesses say they would not have survived Covid-19 without digital tools.

Yet, America is at an inflection point on geopolitical leadership in technology policy. Since the advent of the internet in the 1990s, the U.S. approach to technology has encouraged: private sector-led innovation; keeping the underlying platforms open and borderless; a bottoms-up, multi-stakeholder approach to standards; a balance between fair use and content infringement; balanced liability regimes; a sectoral approach to privacy; and freedom of expression. This policy framework has traditionally been the model for other countries to build their own digital economies.

To continue leading the world, the U.S. must update its own policy approach to the digital economy in a way that protects consumers and citizens, but embraces innovation, an open internet, and the potential economic and societal benefits of new technology for all sectors, businesses of all sizes, and underrepresented voices.

The current lack of a comprehensive digital governance agenda in the U.S. poses challenges for companies operating here. In no area is this more apparent than privacy, where the U.S. is one of few countries without comprehensive federal legislation governing privacy issues, instead relying on a patchwork of state regulations providing guidance ranging from minimal to, in the case of California, comprehensive. More importantly, this lack of a domestic agenda impedes America's ability to advocate for a global digital governance model that reflects values of openness, transparency, and democracy, as opposed to China's governance model of censorship, monitoring, and autocracy.

The digital governance model that becomes prevalent over the next decade will shape America's competitiveness, security, and jobs for the foreseeable future.

> **The digital governance model that becomes prevalent over the next decade will shape America's competitiveness, security, and jobs for the foreseeable future.**

Digital governance encompasses a broad range of issues ranging from cross-border data flows and data storage, to standards, privacy, taxation, cybersecurity, competition, and content moderation. Safe and open cross-border data flows and no requirements for local data storage are widely agreed to by OECD countries and are already in recent trade agreements such as the United States-Mexico-Canada Agreement (USMCA). While USMCA includes a provision on cybersecurity, international disciplines governing cyber must be significantly expanded.

The U.S. government must also significantly expand the resources it devotes to international standards setting bodies, through the State Department and the National Institute of Standards and Technology (NIST). China devotes significant resources to staffing international telecommunications standards organizations, which affords it a significant role in shaping technology standards. The U.S. must increase the resources it devotes to these bodies to ensure the nation has a voice with respect to global standards, particularly in newly evolving technologies like AI. (See the Leading Globally section of this paper for additional discussion of standards setting bodies.)

Two issues that are critical to digital governance, content moderation – in particular, the need to protect children – and competition among technology companies, are outside the scope of this paper, so they will be addressed only briefly. Regarding content moderation, it is essential that the U.S. reach a national consensus that acknowledges the necessity of keeping the internet a safe and credible avenue for gathering and sharing both personal and business information.

The inability of social media companies to stop malicious actors from weaponizing such social platforms, as happened with ethnic violence in Sri Lanka, genocide in Myanmar, as well as extremist rhetoric in the U.S., has

resulted in increased frustration. Following the Christchurch massacre in March 2019, New Zealand's Prime Minister Ardern and France's President Macron arranged a gathering of heads of state and tech CEOs in an attempt to "bring to an end the ability to use social media to organize and promote terrorism and violent extremism." The group issued the Christchurch Call, an agreement between governments and tech companies to eliminate terrorist and violent extremist content online. Forty-eight countries and the United Nations Educational, Scientific and Cultural Organization (UNESCO) have signed onto the call, as well as several tech companies including Google, Facebook, Twitter, and YouTube. The Trump Administration declined to sign, citing First Amendment concerns, but said it was aligned with the agreement's principles. The issue of regulating extremist language online has become more urgent in the wake of the January 6 attack on the Capitol, which was planned publicly on social media. While regulating extremist language online is still under debate in the U.S., it is critical that it be addressed in line with global norms.

As the U.S. seeks to lead on values of transparency, openness, and democracy with other techno-democracies, addressing these issues at home in the U.S. – whether through a legal regime or a more voluntary process – will be critical.

Secondly, there is a great deal of debate surrounding competition policy for America's large technology giants, and competition cases are currently being litigated in the courts. Competition policy in the technology sector must take into account the important need to safeguard consumer protections and promote a business environment that fosters innovation and entrepreneurship, while viewing technology companies' size and impact through a global lens.

While each of these regulatory issues is important in defining digital governance, this paper will focus primarily on the issue of privacy, where an urgent need for federal legislation exists. The issues of taxation and cybersecurity, which depend on international consensus, are addressed in the Leading Globally section of the paper.

Privacy

The lack of a comprehensive national framework for privacy, as well as lingering questions on the taxation of the digital economy, have put the U.S. government on its back foot in negotiations with trading partners around the world. It has also made the U.S. an overly complex regulatory market for its own companies, as well as for technology users.

The U.S. is the only developed country in the world that does not have a comprehensive federal privacy standard governing its data. A comprehensive privacy regime is important to ensure consumer protection and corporate responsibility, while guaranteeing transparency and enforcement. In 2019, the Government Accountability Office (GAO) recommended: "Congress should consider developing comprehensive legislation on internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving internet environment."[52] Since then, several strong privacy bills have been introduced in Congress. In particular, the comprehensive privacy bills proposed by Senate Commerce Committee Chairman Roger Wicker (R-MS), Ranking Member Maria Cantwell (D-WA) and Senator Jerry Moran (R-KS), and bills proposed by members of the House Energy & Commerce Committee, Congresswoman Suzan DelBene (D-WA), and others, are historic in their scope, strength, and sophistication.

NIST is also developing a voluntary privacy framework as a tool for organizations to adopt, identify, assess, manage, and communicate about privacy risks. While this framework will be a useful tool, it is not intended to address the legislative gap in the U.S.

Most Americans have become frustrated by the lack of adequate privacy protection. According to a recent KPMG study, 97 percent of Americans say data privacy is important to them, with 87 percent viewing privacy as a human right.[53]

A federal privacy regime has also become more urgent during the pandemic as more Americans are conducting critical business, like telemedicine, on-

line. Former Federal Trade Commission (FTC) Commissioner Julie Brill, in her recent Senate testimony, pointed out that the lack of a privacy regime in the U.S. has hampered the ability to use health-related data to better respond to the Covid-19 crisis. She highlighted that Covid-19 has disproportionately impacted African Americans and other vulnerable populations.[54] Yet many people in these communities are skeptical about using digital tools to address the crisis due to heightened concerns that personal information collected could be used to violate their civil rights. U.S. privacy law must incorporate measures to protect civil rights and ensure that health and other personal information collected to address the Covid-19 crisis be used for that purpose only.

The Global Perspective

For several decades, the OECD has played a role in promoting respect for privacy as a fundamental condition for the free flow of personal data across borders. The first OECD privacy principles were established in 1980 and have been periodically updated, the latest being in early 2020.[55] The guidelines stress the importance of national strategies for privacy protection, together with improved interoperability between national regimes.

The European Union's (EU) General Data Protection Regulation (GDPR) has had tremendous influence on global legal norms for privacy and data protection. The GDPR, which went into effect in 2018, regulates the processing of personal data of individuals who are EU data subjects, including cross border data transfers. As an EU regulation, the GDPR applies directly as law to EU member nations. The GDPR also has extensive extraterritorial provisions that apply to processing of personal data outside the EU, regardless of place of incorporation or geographical area of operation of the data controller/processor. A number of non-European countries have adopted regimes that are GDPR compatible, including South Korea, Australia, New Zealand, Brazil, Chile, and Japan, which has updated its laws to be more aligned with GDPR and established "reciprocal adequacy" agreements with the EU.

APEC Cross Border Privacy Rules ("CBPR") is another major regional framework regulating transfer of personal data between APEC member nations. It is a voluntary accountability scheme that initially requires acceptance at

the country level, followed by independent certification by an accountability agent of the organization seeking to join the scheme.

In 2016, the U.S. and the EU established a "Privacy Shield" framework to provide companies on both sides of the Atlantic a mechanism to comply with data protection requirements when transferring data between them. The Privacy Shield was struck down by Europe's highest court in July 2020, based on findings that the protection of personal data in the U.S. was not "essentially equivalent" to the European legal order. While this decision ("Schrems II") casts a shadow of uncertainty over the future of EU-to-U.S. data flows, it also provides a unique opportunity to bring together the EU, U.S., and other like-minded democratic nations to further the protection of personal data while preserving a common vision for an open, transparent, and democratic internet.

In the absence of federal privacy legislation, states have taken matters into their own hands. California passed the California Consumer Protection Act (CCPA), which took effect in January 2020 and incorporates the core privacy rights that exist in GDPR and other global privacy laws.

Recognizing that more was needed to ensure that the responsibility for protecting privacy was borne by companies and not just by individuals, the proponents behind CCPA introduced the California Privacy Rights Act (CPRA) initiative, which overwhelmingly passed into law this past November. CPRA requires companies to uphold additional obligations from GDPR, including to engage in data minimization and purpose limitation, and to assess the risk of their data collection and use practices. Further, CPRA introduces protections for sensitive data and children, and provides individuals with the ability to opt-out of advertising activities of large companies on third-party websites.

Washington state has also advanced the Washington Privacy Act (WPA), a bill that would build upon the current global standard for privacy protection set by GDPR, an updated version of which has been introduced again in the most recent legislative session. Several other states are currently considering similar legislation.

The U.S. has traditionally sought a balanced approach between trade, privacy, and security.[56] Some in the U.S. regard the GDPR as more restrictive, thus offering a higher level of privacy protection, while the CBPR is viewed as more conducive to business. During the Covid-19 pandemic, however, American concerns have become more urgent. That, together with the fact that GDPR is increasingly becoming the de facto global privacy standard, and with the invalidation of the Privacy Shield, many companies have scrambled to ensure they can meet European privacy norms to be able to sell in the EU.

The U.S. should move rapidly during the next congressional session to adopt federal privacy legislation that adheres to principles of data portability, interoperability, transparency, and user consent, and is thus GDPR compatible. Adopting such legislation would avoid a confusing patchwork of standards across different states, move the world toward stronger privacy standards, and promote a more robust environment for cross-border transfers of data to grow exponentially. The OECD should also be engaged to promote globally interoperable solutions to these issues.

Upgrading U.S. Technological Competitiveness

The U.S. dominated technological innovation for decades, leading the world into a highly connected economy, powered largely by U.S. innovation. While the U.S. continues to be a leader in the digital economy, China's national technology drive, as seen in its Made in China 2025 initiative,[57] its growing budget for research and development, and its aggressive drive to dominate technology market share in third countries, have challenged U.S. technology leadership. These challenges should awaken the U.S. from complacency and drive a coordinated and targeted federal effort to ensure U.S. technological competitiveness in the coming decades.

The U.S. is competing in a global landscape, with many countries using coordinated industrial policies to advance their industries in the technology race. Given China's subsidization of its R&D and technology industries, the playing

field is not level. A key element to addressing the China technology challenge is to strengthen U.S. competitiveness. While the U.S. technology private sector remains strong and innovative, it must be bolstered by a broad government effort to strengthen the U.S. scientific and technological base and adopt policies that will allow the U.S. to maintain global technology leadership.

Just as the U.S. mobilized to address the strategic threat of the Soviet Union and the economic threat of Japan, it can similarly mobilize a comprehensive effort to advance U.S. competitiveness. In addition to identifying and implementing the right policies, U.S. values are an important element of U.S. competitiveness. The U.S. approach to competitiveness should advance an affirmative narrative of openness, transparency, and democracy, and the strategy should be broader than just competition with China, though that is key.

Such a strategy should include several policy priorities: increasing federal support for innovation, including funding for basic R&D and early stage technologies; targeting support for a limited group of critical technologies; creating a path for immigration that is in the U.S. national interest, recognizing that openness strengthens U.S. innovation; upgrading our government bureaucracy for a digital age; and finally, creating a Digital Marshall Plan to promote U.S. technology – and technology policy – abroad.

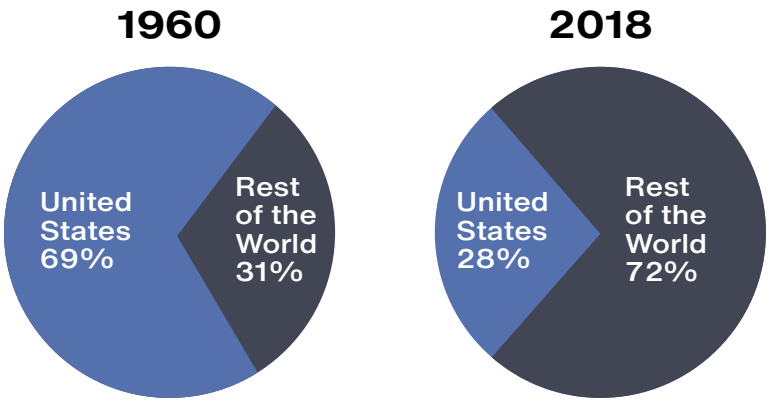
Federal Support for Research and Development (R&D) Needs a Boost

The U.S. became a global leader in R&D in the 20th century, funding as much as 69 percent of annual global R&D in the 1960s. But by 2018, the U.S. share had fallen to a little over 25 percent. This decline is not the result of a reduction in U.S. R&D investments, but rather increases in investments by other countries, reflecting an increasingly competitive global innovation landscape.

The global concentration of R&D performance continues to shift from the U.S. and Europe to Asia. Japan, Singapore, South Korea, and Taiwan have all seen science and technology as essential to economic security. For example, South Korea increased spending on R&D[58] as a percentage of GDP from 2.1 per-

cent in 2000 to 4.5 percent in 2017. China increased spending on R&D from $13 billion in 1991 to $410 billion in 2016 – and now accounts for roughly 20 percent of global R&D.[59] In contrast, U.S. government spending on R&D as a percentage of GDP fell from a high of 2.25 percent in 1962 to 0.6 percent in 2019.[60]

Figure 1
U.S. Share of Global R&D



Sources: 1960: CRS analysis of U.S. Department of Commerce, Office of Technology Policy, *The Global Context for U.S. Technology Policy,* Summer 1997. 2018: CRS analysis of Organisation for Economic Co-operation and Development (OECD) data, Main Science and Technology Indicators, OECD.Stat.
Notes: Rest of the World includes the members of the OECD (less the United States), Argentina, China, Romania, Russia, Singapore, South Africa, and Taiwan. R&D expenditures by other countries are not included but are likely to be small in relative terms. In estimating total global R&D, CRS used the most recent year's reported R&D expenditures for three countries (Argentina, Singapore, and South Africa) that had not reported data for 2018.

Moreover, the federal government's R&D spending as a share of overall U.S. R&D spending has been on the decline. After 1980, U.S. R&D was increasingly conducted at private facilities and motivated by business concerns responding to market stimuli and tax incentives. Rather than serving long-term strategic objectives such as nuclear deterrence or space exploration, private sector R&D has focused on shorter-term goals, such as product development and process improvement. Private-sector R&D investment has risen, but it is not a substitute for federally-funded R&D directed at national economic, strategic, and social concerns. U.S. leadership in science and technology is at risk because of a decades-long stagnation in federal support and funding for research and development.

Year	U.S. Business R&D Spending (% of Total)	U.S. Government R&D Spending (% of Total)
1980	47.6	46.5
1995	59.4	35.5
2000	69	26.2
2005	63.3	30.8
2010	56.9	32.6
2015	62.5	25.3
2018	62.4	23

Source: UNESCO and OECD historical data on R&D expenditure

Increased federal support for R&D, particularly at the level of basic research, is an important and appropriate step to bolster the U.S. innovation ecosystem in a new, more competitive global environment. The bulk of federal funding for R&D is for basic and applied research, which often require consistent and substantial funding over long periods, and is not easily replaced by funding from the private sector.[61] In the past, basic research funded by the federal government has contributed to innovation for computer chips, the internet, and GPS. This is important long-term foundational research that the private sector doesn't have the capacity to undertake. Even as U.S. technology companies lead research in AI and other emerging technologies, history has shown that U.S. companies have relied on basic research funded by the federal government to advance their own research and bring technology to market.[62]

To remain competitive, both domestically and globally, studies have shown that the U.S. needs to increase federal R&D spending at least to 1980s levels, or doubling as a share of GDP.[63] As it faces increasingly fierce global competition, the U.S. risks ceding its edge to breakthroughs that occur elsewhere in the world or losing U.S. researchers to other countries that are funding cutting-edge projects not funded in the U.S. Further, to the detriment of individuals around the world, there is a risk of innovative global technologies being built without the values that Americans, among others, believe in and aspire to.

In addition to broad increases in the U.S. research and development budget, the U.S. needs to fund targeted support for a limited group of critical technologies. Past federal commitments to prioritize so-called industries of the future, including a commitment to double non-defense R&D spending on AI and quantum information science (QIS) by 2022, are a step in the right direction. Another important initiative is the CHIPS Act, a bill introduced in June 2020, which includes tens of billions of dollars in research and manufacturing investments and incentives to strengthen U.S. leadership in semiconductor technology, which is critical to national security and economic strength. The bill was passed on January 1, 2021, as part of the National Defense Authorization Act (NDAA) as Title XCIX, "Creating Helpful Incentives to Produce Semiconductors for America," which authorizes federal incentives to promote semiconductor manufacturing and federal investments in semiconductor research. Federal government investment in semiconductor research is currently only a fraction of total semiconductor R&D in the U.S. and has been relatively flat as a share of GDP for many years; and U.S. semiconductor manufacturing growth has lagged other countries. This legislation would level the playing field between the U.S. and other countries that provide significant incentives to their semiconductor industries.

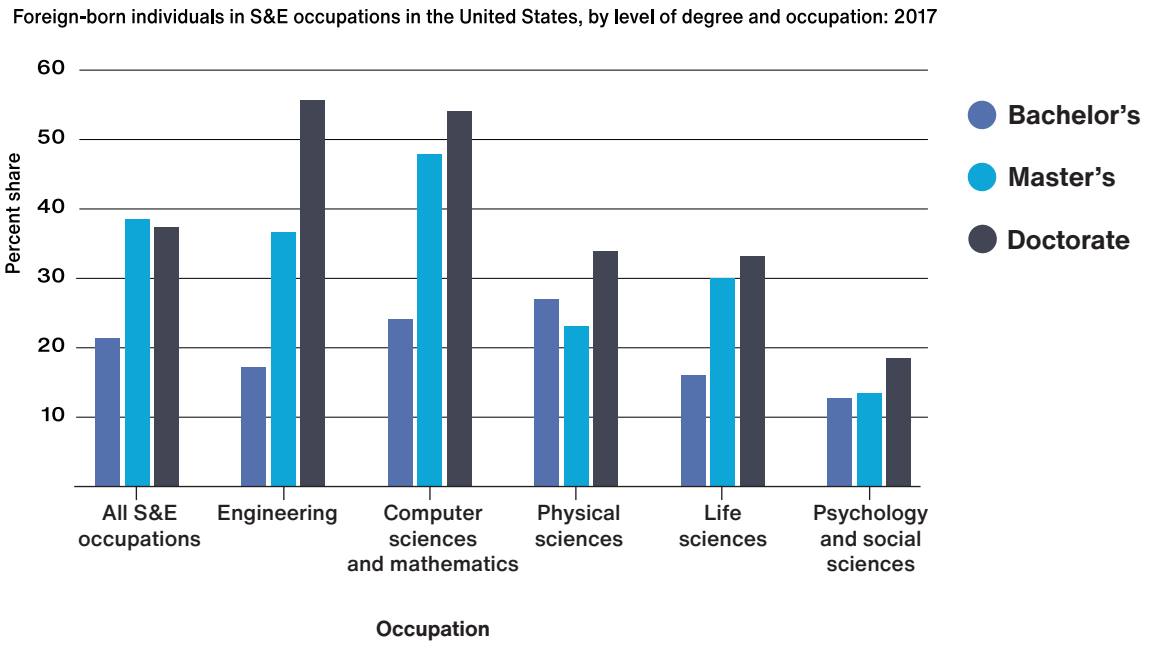
Fortunately, there is strong bipartisan support in Congress to restore U.S. federal R&D funding to 1.2 percent of GDP, as well as develop targeted R&D funds for specific critical technologies.[64] If this funding is approved, it would mark an important and meaningful step in reinvigorating the U.S. innovation ecosystem.

Immigrants Are a Vital Part of the U.S. Innovation Ecosystem

As many experts and historians have recognized, immigration policy is really innovation policy. Openness to global talent has facilitated America's innovation enterprise in both commercial markets and military applications and has been a strength of its system.[65] The debate on immigration needs to be refocused on its contribution to the nation's well-being broadly, as well as its importance to the tech sector.

Foreign-born workers—ranging from long-term U.S. residents with strong roots in the U.S., to more recent immigrants—account for 30 percent of workers in science and engineering (S&E) occupations. In many S&E occupational categories, the higher the degree level, the greater the proportion of the workforce who are foreign born. More than one-half of doctorate holders in engineering, computer science, and mathematics occupations are foreign born (see chart below). In comparison, about 18 percent of the overall population and 17 percent of the college graduate population in the U.S. are foreign born.

Figure 9: National Science Board
Science & Engineering Indicators | NSB-2020-01



Source: https://ncses.nsf.gov/pubs/nsb20201/u-s-s-e-workforce

Welcoming immigrants into the U.S. technology sector is important because it strengthens American society, and because of the skills many of these individuals bring. However, it is essential to consider possible security risks posed by some Chinese students and scientists. Security challenges and state-sponsored espionage via the U.S. education system and research labs are real and need to be addressed. But the response should be to increase scrutiny of our screening processes, not to undermine longstanding values

related to openness, including immigration, which is crucial to the U.S. competitive advantage in innovation.

Immigrants have made significant contributions to the U.S. innovation and entrepreneurship ecosystems. The National Foundation for American Policy finds that 55 percent, or 50 of 91, of the country's $1 billion startup companies had at least one immigrant founder.[66] Immigrants make up roughly 15 percent of workers in the U.S., yet they are 80 percent more likely than native workers to become entrepreneurs, according to the study.

First- and second-generation immigrants are launching businesses across the spectrum, from small sandwich shops with one or two employees, to major tech firms with thousands of workers.[67]

Yet, the U.S. has seen a sharp decline in visas for both foreign students (-44 percent) and specialty workers (-18 percent) since 2015.[68] Actions by the Trump Administration to limit H-1B visas have hampered tech firms that rely on top global talent. The denial rate for applicants trying to extend their visas grew from 4 percent in 2016 to 12 percent in 2018 and to 18 percent in the first quarter of 2019.[69] The Trump Administration also proposed ending the work authorizations for H-4 visa holders (the spouses of H-1B visa holders), making it yet more difficult to attract and retain talent.

In addition, in June 2017, the Department of Homeland Security (DHS) proposed ending the International Entrepreneur Rule, which provides temporary residency to foreign entrepreneurs starting a business in the U.S. Other countries, such as Australia and Canada, are using these developments to lure talent.

In October 2020, the Trump Administration introduced two regulations to make it harder for foreign skilled workers to qualify for H-1B visas and harder for U.S. companies to afford to hire them.[70] One regulation would have narrowed the definition of a "specialty occupation" and the number of occupations that would qualify. Another regulation would have significantly increased the required wage rates employers would have to pay and make it more costly for employers to hire foreign skilled workers. However, these

rules were set aside by a U.S. district court on procedural grounds.

> Restrictive immigration regulations could force companies to move high-skilled and high-paying jobs offshore.

Restrictive immigration regulations could force companies to move high-skilled and high-paying jobs offshore. Research from earlier this year indicates that skilled immigration restrictions may have "secondary consequences that have been overlooked in the immigration debate: multinational firms faced with visa constraints have an offshoring option, namely, hiring the labor they need at their foreign affiliates."[71] This would be yet another setback in the development of America's innovative capacity.

In December 2020, the Senate passed an amended version of the Fairness for High Skilled Immigrants Act (S. 386/H.R. 1044).[72] While much remains to be worked out between the House and Senate versions, fixes such as eliminating per-country caps on employment-based immigrant visas and making it easier for H1B workers to change jobs are positive developments. Congress and the Administration should work together to facilitate the ability of U.S. companies to employ H-1B foreign workers, as well as obtain L-1 visas for transfers for intracompany executive-level workers, and H-4 visas for dependents of H1B workers, where they are needed in the U.S. economy, and to move forward on comprehensive immigration reform that is integral to our country's competitiveness and national security.[73] President Biden's first moves turned immigration policy in the right direction, recognizing the value that immigrants bring to American society and establishing a more humane approach to immigration. Additional steps are needed, however, to ensure the right policies are in place to support innovation and the U.S. technology ecosystem.

Protecting Our Technology

Rather than pursuing a strategy of protecting an expansive range of technologies, the U.S. is best served by identifying a limited number of key technologies, together with certain data that will fuel critical new innovation and insights and protecting those very well – a "small gardens, high walls" technology strategy.

Current and Future Export Controls

In May and August 2019, the Department of Commerce added Huawei and its affiliates to the "Entity List" of foreign companies to which it is illegal for Americans to provide a good or service without a license.[74] The orders were intended to prevent essential American-made semiconductor inputs from getting to Huawei directly and electronic design automation (EDA) tools to its subsidiary chip designer HiSilicon, ultimately hampering Huawei's ability to produce telecom equipment.[75]

The Department of Commerce implemented additional rounds of export controls in May and August 2020.[76] Under the foreign-produced direct product (FDP) rule, the Commerce Department effectively put new limits on sales by American companies of a new part of the semiconductor supply chain—manufacturing equipment—to chipmakers overseas, also rocking the market for dominant U.S. manufacturers.

While these controls did inflict some pain on the target, they also had negative side effects. Within the U.S., the controls at times caught technology that was widely available in the global market and promoted foreign products over U.S. products in the global market. The controls also created great uncertainty in the investor and research communities. Unilateral controls also disadvantaged U.S. companies, since foreign companies were not subject to the same controls. The Center for New American Security asserts that "unilateral controls create incentives to invest in the development and production of the items outside of the U.S. and do not necessarily restrict their ultimate transfer to countries of concern—while harming the industrial base of the country imposing the control."[77]

At the same time, an export control regime that depends on broad unilateral controls and granting company exceptions raises the potential for mismanagement. Government officials have to decide on exceptions, arising from company petitions, on a case-by-case basis, creating concerns over cronyism, non-transparency, and discrimination.[78]

In China, the controls empowered voices that called for more drastic state

measures to counter U.S. technological dominance. Among customers of U.S. technology in China, the controls exacerbated a perception that the supply of U.S. technology is unreliable and should be designed out of new products.

Export controls should be targeted and enforced in concert with U.S. allies.

The processes for implementing U.S. export controls should be adjusted in several ways. The 2018 Export Control and Reform Act (ECRA) made progress in this direction. ECRA directed the Commerce Department's Bureau of Industry and Security (BIS) to conduct an interagency review process to identify so-called "emerging and foundational technologies."[79] These are intended to be technologies that historically have not been subject to export controls under multilateral regimes, but are nonetheless essential to U.S. national security. In 2018, BIS issued an Advance Notice of Proposed Rulemaking (ANPRM) seeking comment on criteria for identifying emerging technologies that are essential to U.S. national security. The ANPRM listed 14 categories, including artificial intelligence, quantum technology, robotics, and advanced surveillance technologies. Once identified as an emerging technology, they would be open to control by BIS rules. Moreover, investment in this area of technology would trigger mandatory filings under the Foreign Investment Risk Review Modernization Act (FIRRMA) under some circumstances. Along with a companion effort around foundational technologies, which closed its public comment period in October 2020,[80] these controls are a key part of the strategy to identify and protect critical U.S. technology – to create high walls around small gardens.

Export controls should not be placed on long-established technologies that are available outside the U.S., or on published technology and information sources, even if they are among potential "emerging" technologies. These controls would allow foreign competitors to take market share from U.S. companies, further undermining U.S. economic security and global digital leadership.

Finally, export controls should be targeted and enforced in concert with U.S. allies. However, it is a fair criticism that processes like those in the multilateral Wassenaar Arrangement on Export Controls for Conventional Arms

and Dual-Use Goods and Technologies move too slowly. The U.S. can try to thread the needle by seeking out a more targeted approach to export controls with like-minded countries.[81] This would prevent China from accessing the technology from other countries and allow countries to jointly implement controls as part of a broader China strategy developed in concert with allies.

Foreign Technology Investment in the U.S.

There has been increasing concern in recent years that the Chinese government has attempted to obtain U.S. technology through joint venture investments with U.S. companies or through investments in start-up companies. The Committee on Foreign Investment in the United States (CFIUS) is an inter-agency committee of the U.S. Government that reviews the national security implications of foreign investments in U.S. companies or operations. While not always the case, Chinese investments in certain U.S. industries have been subject to CFIUS reviews.

In 2018, Congress passed FIRRMA to modernize CFIUS and close gaps that allowed investments in sensitive U.S. industries to avoid CFIUS review. In particular, FIRRMA[82] expanded CFIUS to include jurisdiction over non-controlling investments in sensitive industries from a U.S. national security perspective – critical technology companies, critical infrastructure companies and companies managing large pools of personally identifiable information on U.S. citizens. While FIRRMA is certainly not intended to only apply to China, concern over the increasing use of Chinese joint ventures into which U.S.-origin technology is transferred, Chinese low-level investments in U.S. start-up technology companies, and Chinese deals potentially being structured to circumvent CFIUS, were significant considerations driving bipartisan support for the legislation.

Securing the Information and Communications Technology Supply Chain

Even before Covid-19, U.S. policymakers were giving increased attention to securing the U.S. supply chain, including in the technology sector. The Information Technology Industry Council (ITI) summarizes key federal actions since 2014,[83] including:

- 2019: Executive Order 13873 empowers the Commerce Secretary to prohibit or mitigate information and communications technology and services (ICTS) transactions that pose risks and take a "case-by-case, fact-specific approach" to determine what transactions will be prohibited or subject to mitigation. The proposed rule does not identify specific technologies or participants. Commerce issued an interim rule on January 14, 2021, identifying six foreign adversaries, including China and Russia, and allowing Commerce to create additional processes to assess transactions.[84]
- 2019: A Federal Communications Commission rule forbids use of Universal Service Fund (USF) subsidies for the purchase of equipment from Huawei and ZTE and provides reimbursements to small and rural carriers who may have to replace such equipment as a result.
- 2018: The Department of Homeland Security's National Risk Management Center (NRMC) established the ICT Supply Chain Risk Management (SCRM) Task Force, a U.S. public-private supply chain risk management partnership, with the critical mission of identifying and developing consensus strategies that enhance ICT supply chain security.
- National Defense Authorization Acts (NDAA): Each year, NDAA added requirements to strengthen supply chain security, including banning certain products from Chinese companies and in certain use cases in the U.S.

While the executive order and Commerce's proposed regulation seek to close the gaps on transactions that ECRA or CFIUS would not cover, there is concern that they are overly broad and heavy-handed and create uncertainty in the market. The success of U.S. technology companies depends greatly on the health and vitality of suppliers in other nations and the ability to trade with them.[85] The U.S. government must address security concerns with a comprehensive, whole-of-government approach to ensure consistency among the numerous government and public-private initiatives focused on supply chain security.[86]

U.S. technology companies have long advocated for approaches to supply chain security to be country-agnostic, establishing objective evaluation criteria to block or mitigate transactions, rather than blanket country restrictions.

Some advocates have asserted that the conflation of national security with economic protectionism will only serve to hurt U.S. companies in the long run, encouraging the same actions by other countries that want to limit market access to U.S. competition.

China plays a big role as both a supply and demand hub in global value chains, and U.S. measures to secure its own ICT supply chain should not ignore this. As with the iPhone and other examples,[87] it is clear that the information and communications technology supply chain will not return to the U.S. in full. However, U.S. policymakers can map supply chain networks of national significance,[88] including for semiconductors and associated high-technology industries, and then work with allies to build out a trusted supply chain framework. This framework, combined with carefully targeted export control measures, is critical to protecting key U.S. technologies.

Other Thoughts on Identify and Protect

Shoring up U.S. cyber defenses tops the list of policies that are key to protecting U.S. technologies. There are many recommendations[89] in this space, including for the NTIA, in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA), to undertake a comprehensive review of core internet vulnerabilities to begin the remediation and removal of technologies and entities compromised by China and to strengthen the federal government's ability to secure critical infrastructure and respond to 21st century threats. Much work has been done already, including the development of the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) for its suppliers.

Similarly, on personnel, though the right immigration policies in science and engineering fields are vital to America's innovation ecosystem, the U.S. should find better methods to screen individuals and university funding sources related to early-stage technologies and other technology areas deemed essential to national security.

Finally, while efforts by new U.S. entities like In-Q-Tel, a CIA-funded venture capital firm, to invest in startups[90] in areas like AI and machine learn-

ing, data analytics, and autonomous systems are positive, they may not be enough to counter China's venture capital attention to early stage technology. Congress should incentivize continued venture capital investment in America's most innovative start-ups.[91] For example, the bipartisan New Business Preservation Act, introduced by Sens. Amy Klobuchar (D-MN), Chris Coons (D-DE), Tim Kaine (D-VA), and Angus King (I-ME), builds on the previously successful State Small Business Credit Initiative (SSBCI) by establishing a program, administered by the Treasury Department, to allocate $2 billion to states on a population basis to attract private venture capital. It would offer a one-to-one match of federal dollars with venture capital investment in promising startups, particularly in states outside the major venture capital centers.[92]

U.S. Government Structure Should Prioritize Digital Policymaking

While many parts of the U.S. government play key roles in formulating policy for the digital economy, each has different equities and controls only pieces of what could make up a full digital strategy. To be an effective leader of democracy in a quickly advancing world, the U.S. government bureaucracy must prove itself willing to evolve with the times.[93]

In 1976, Congress established the White House Office of Science and Technology Policy (OSTP) to provide the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources. Since its establishment, OSTP has varied in leadership and strength and has not played a strong role in driving a coordinated global digital strategy for the U.S. The move to elevate OSTP to a cabinet level agency is a welcome step in the right direction.

Even before OSTP was established in the Executive Branch, the Office of Technology Assessment (OTA) served as a nonpartisan body to advise Congress on the implications of science and technology applications. However, it

closed in 1995, and some argue this closure reduced the ability of Congress to grapple with technologically complex issues, not to mention helping to increase Congress' dependence on lobbyists.[94] Having a reliable information source on technology for members of Congress will be critical as it seeks to legislate on a range of digital issues.

America's allies have seen the need to focus digital policy efforts across their governments. Japan, for example, has plans to establish a digital policy agency.[95] This agency will focus on promoting e-governance and improving coordination on policymaking for information technology and may be led by a figure drawn from the private sector.

The U.S. federal government has no shortage of agencies devoted to science and technology, but what is lacking is an overarching body to drive coherent and comprehensive digital economy policy efforts and a forward-leaning global strategy. An Office of Global Digital Strategy in the Executive Office of the President (EOP) Office, like the Office of the U.S. Trade Representative, with its lean and expert staff, would go a long way to coordinating across various government agencies, weaving together disparate pieces of technology policymaking. Such an agency would coordinate domestic policy and regulatory issues, lead U.S. engagement in a coalition of techno-democracies, and host classified, private sector advisory committees to advise on both global competition and innovation cooperation with other countries.

Playing Offense, Not Just Defense: A Digital Marshall Plan

The U.S. must also focus on how to increase competitiveness in global markets. The Chinese government invests billions in its technology companies, positioning them to win sales through subsidized government financing, which makes it difficult for U.S. technology companies to compete on fair terms, and leaves developing countries without an option to purchase an open, democratic internet.

In 2015, China launched the Digital Silk Road, investing $200 billion in a global digital infrastructure.[96] This effort is a subset of China's larger Belt

> The U.S. must launch a "Digital Marshall Plan."

and Road Initiative, a government- sponsored global infrastructure initiative with $340 billion invested to date.[97] The Chinese government is using these resources to offer subsidized loans to its companies, including Huawei, as well as foreign assistance grants to government customers, to capture digital market share, especially in the developing world. The effort's reach is broader than just equipment – when developing countries buy Chinese equipment, they receive the tools to censor and control their internet, while leaving their networks vulnerable to Chinese government cyber theft and interference.

In addition to seeking agreements from other countries to remove Huawei equipment from their telecom networks, the U.S. needs an offensive strategy[98] that allows U.S. companies and workers to compete on a level playing field with Chinese companies that have received government subsidized financing, while offering real alternatives for underdeveloped countries looking for affordable, reliable technology and the opportunity to purchase internet infrastructure consistent with an open, accountable, and democratic internet. The U.S. must launch a "Digital Marshall Plan" to make the financing of American digital infrastructure in the developing world a strategic priority. As part of this initiative, the U.S should also provide technical assistance to develop internet regulations that allow open commerce, respect for privacy and protection of human rights.

The new International Development Finance Corporation (IDFC) should play a large part in this initiative. The IDFC 2020 budget is $60 billion, with only $1 billion of investments to date, and only one small project in the telecommunications sector.[99] Its next budget should earmark $50 billion for digital exports, with an emphasis on matching financing for U.S. companies competing with Huawei in areas like data center storage and cloud networking.

A second leg of the U.S. export financing toolbox is the U.S. Export-Import Bank (EXIM) which provides financing to support U.S. exports. Part of the Digital Marshall Plan should include easing the requirements for U.S. companies to access EXIM financing, especially in the case of companies competing with Chinese technology companies. EXIM should be directed to

implement "national interest" waivers of strict U.S. content requirements for export support in key projects and change its content methodology to calculate content to include the value of intellectual property (IP) developed in the U.S. Finally, part of this plan should involve earmarking funds from the U.S. Agency for International Development (USAID) for technical and regulatory training for the digital sector.

U.S. embassies in foreign countries provide vital advocacy support for U.S. companies selling in those markets. The U.S. Department of Commerce has a Digital Attaché program that includes trained staff in 12 key foreign markets who support U.S. companies, including by navigating foreign digital policy and regulatory issues, and are part of Commerce's comprehensive effort to address 21st century trade barriers and help the digital economy thrive. The State Department runs a similar modest program for Foreign Service Officers. Given the extremely rapid expansion of digital exports to every country in the world, these programs should be expanded, with training in digital policies and regulations in most key embassies.

Invest in America Summary of Recommendations

Access and Inclusion

- **Education and Training:** Launch a federal initiative to ensure that digital skills are taught in all K-12 schools nationally.
- Increase federal spending on digital training programs, especially for workers who are unemployed or in low-wage jobs. Programs should be designed to be fully inclusive of women, people of color, and individuals from other marginalized groups, which are traditionally under-represented in digital training. Partner with MSIs to help make these programs more accessible. Companies should be incentivized to expand their training programs.
- Continue the trend of expanding federal support for apprenticeship programs and provide tax credits to businesses to further incentivize their

participation. Pass the National Apprenticeship Act of 2020, with amendments to focus on digital apprenticeships, and ensure that the apprenticeships are accessible to workers from marginalized communities.

- Enact federal legislation to make community college more affordable for low-income families, as well as create incentives for companies to partner with community colleges on digital skills training.
- Increase funding to MSIs and HBCUs for STEM and computer science training, to promote apprenticeships for their graduates.
- **Equipment and Broadband:** Make a historic investment in America's connectivity to close the digital divide, including by subsidizing internet access and equipment access for low-income families. Upgrade the U.S. broadband network. Pass the Accessible Internet for All bill, which allocates $100 billion for nationwide broadband and programs to make the internet affordable for low-income households.
- **Spectrum:** Free up additional spectrum for wireless use.
- **Net Neutrality:** Enact federal legislation to balance consumer protection interests with incentives to business to create internet access for all.

Digital Governance

- **Privacy:** Pass federal privacy legislation during the next congressional session that is GDPR compatible and embodies principles of data portability, interoperability, transparency, and user consent.
- **Content Moderation:** Endorse the Christchurch Call and build on this with a techno-democracy coalition to develop rules around disinformation and extremist content online.

U.S. Technological Competitiveness

- Double current U.S. federal R&D spending on basic research to 1.2 percent of GDP.
- Establish a process to identify a limited group of critical technologies that would benefit from targeted support, such as is envisioned in the CHIPs Act.

- Return H1B and related visa issuances to previous levels and move forward on visa reform that reflects U.S. values of openness, recognizes immigrant contributions to our innovation ecosystem, and incorporates adequate screenings for access to sensitive and early-stage technologies.
- Protect U.S. technologies with a "high-walls, small gardens" approach to export controls, supply chain security, and foreign investment screening that is well-coordinated with industry.
- Establish a Global Digital Policy Office in the Executive Office of the President to coordinate and advance strategy across all government agencies for both U.S. domestic and foreign digital policy and strategy.
- Appropriate $50 billion in funding for a Digital Marshall Plan to be administered through the IDFC and USAID, to enable U.S. companies to win globally against heavily subsidized competitors like China and give developing countries the opportunity to purchase equipment consistent with a democratic internet. Update EXIM's qualification criteria to allow for "national interest" waivers of EXIM's export content requirements and change its U.S. content methodology to include the value of IP.

Part II: Leading Globally

As the internet has evolved, digital technology has become an ever more critical part of the global economy. The economic impact of the internet was estimated to be $4.2 trillion in 2016, making it equivalent to the fifth-largest national economy. In 2018, digitally deliverable service exports amounted to $2.9 trillion, or 50 percent of global services exports.[100] However, the benefits from this activity have been distributed unequally, with more than half the world's citizens having little or no access to the internet, limiting their ability to participate in the increasingly important digital economy.[101]

Yet, international collaboration governing the digital economy has lagged. While small groups of countries have negotiated agreements covering some pressing issues of today's digital economy, coherent global digital governance remains largely elusive. The U.S., which has historically been the architect of global governance, was absent from the global stage during the Trump Administration as this digital transformation escalated.

With legitimate concerns over privacy and cybersecurity, countries have responded to the global regulatory vacuum by enacting a wide range of regulatory and trade measures which restrict data flows, limiting the ability of their citizen to benefit from the internet, impeding the ability of American companies to do business in their borders, and potentially undermining U.S. national security.[102]

Of greater concern are countries like China, which use digital restrictions to censor the internet and to monitor and control their citizens. When China sells its digital infrastructure equipment to developing countries, it also exports its internet regulatory principles, including the means to censor, monitor, and suppress citizens.[103]

Now is the time for the U.S. to position itself as a global digital leader in the 21st century. It must assert its leadership to create consensus around a global digital governance agenda; and it must unite its allies on issues such as digital privacy, taxation, standards, and protection of key technologies. This

consensus is needed to ensure that the world doesn't splinter into different regulatory blocs, creating havoc for global digital commerce and stifling global growth. U.S. leadership is particularly needed to develop standards for new technologies, including for artificial intelligence and facial recognition, which will protect consumers and human rights. Most importantly, U.S. leadership is needed to ensure that the American vision of an internet that is open, accountable, and democratic prevails globally, and that countries around the world have access to that internet.

As discussed in the first section of this paper, the largest piece of the U.S. strategy to become a global digital leader starts by **Investing at Home,** including addressing the inequalities in technology access, significantly increasing federal R&D spending, protecting key technologies, passing federal privacy legislation, and energizing global competitiveness through a Digital Marshall Plan.

The second priority is **Leading Globally**. The most important step for the Biden Administration will be to repair relationships with its allies and develop a coordinated approach to address China's policies. The Biden Administration will need to shift from the ill-conceived unilateral approach of the Trump Administration, and work with its allies to develop a global digital trade and governance agenda, based on shared values, including a vision of an open and democratic internet. A new strategy should involve a multipronged series of international collaborations, starting with an alliance of those countries most aligned with the U.S., the tech-democracies, and then branching out to include agreements with other countries.

Setting a New Approach to China

Parallel to the rapid growth of the global digital economy has been the growing role of China in this sector. Over the past quarter century, the U.S. has been the undisputed global technology leader. However, China's rapid rise as a technology power poses new challenges for the U.S. and the global community. By 2030, China is poised to overtake the U.S. to become the leading

global spender on research & development (R&D).[104] And China has surpassed the U.S. in deployment of several key technologies, including artificial intelligence applications like facial and voice recognition, 5G technology, and digital payments, and is advancing quickly in the development of other areas of AI, quantum computing, and other critical technologies.

Bolstered by plans like Made in China 2025, a strategic plan to make China one of the world's most innovative countries by 2025 and a leading global science and technology power by 2049, China has worked to move up the manufacturing value chain and claim its place as a technological power in the world. In addition to large investments in R&D and technology development, the Chinese government has also used a wide array of subsidies to promote investment in its domestic technology companies and subsidize their exports, allowing its companies to greatly expand their global market share at below market costs. For example, in 5G, China's subsidization of Huawei has led to the rapid deployment of their products globally. This has translated into market share with Huawei leading the global mobile base station market in 2020 with a total share of 28.5 percent, up from 27.5 percent in the previous year.[105]

At home, the Chinese government has imposed investment and ownership restrictions on U.S. technology companies in China, and cajoled or required the transfer of American technology and intellectual property to Chinese enterprises.[106] In many cases, China then closed its market to foreign technology, allowing its companies to grow in their protected domestic market.

There is bipartisan agreement that the U.S. needs to change its approach to the U.S.-China relationship. Unfortunately, U.S. policies towards China over the past four years have been scattershot. Furthermore, tariff policies have not yielded structural changes in China that would benefit the U.S. economy, yet they have cost Americans billions of dollars. While the U.S. government has imposed expanded and useful export controls against Huawei, ZTE, and other Chinese companies, these have been implemented without sufficient public consultation or a comprehensive strategy. And all of these actions have been taken by the U.S. unilaterally, without coordination with our allies.

Even with wide bipartisan agreement on the threat China poses to U.S. global leadership on technology, U.S. policymakers diverge on whether our China strategy should move us toward complete decoupling with China, or a more nuanced and targeted, but still aggressive, set of policy responses. Complete decoupling, with no dialogue channels or business relationships, carries significant national security and economic implications. For example, the Boston Consulting Group estimated that a full decoupling with China would reduce the U.S. semiconductor sector's revenue by 37 percent and lower its global market share to 30 percent; by contrast, China's market share would rise from 3 percent to 31 percent.[107] But beyond U.S. commercial losses, decoupling in all areas means U.S. government and its private sector have less visibility into what China is doing and capable of, putting the U.S. at a disadvantage and making it harder to influence China. More strategic assessments are needed to determine where to maintain interdependence with China and where to surgically focus protection of U.S. technologies and market share.

Some have asserted that interdependence with China is a vulnerability. While this may be true in some areas, it is not for all. Leading thinkers have put forward new paradigms for the U.S.-China relationship, such as "principled interdependence"[108] or "limit, leverage, and compete,"[109] which involve cooperating where possible, yet addressing and limiting the risks posed by China's high technology drive. U.S. attempts to protect the country from the risk posed by China need to be done as part of a larger strategy, in consultation with companies and other stakeholders, and in collaboration with allies. The recent U.S. decision, for example, to ban TikTok and WeChat, was done in a rushed, arbitrary way, using emergency economic authority, only to be overturned in court.[110] The U.S. should develop objective standards by which to evaluate potential economic and security threats to American technology and especially American data.

The U.S. must be clear-eyed about the challenges that China poses and address them accordingly. The U.S. must also stand steadfast by its commitment to human rights and other core U.S. values. At the same time, it should

build on areas of common interest with China. The two countries should identify shared interests, for example on the environment, healthcare, and nuclear proliferation, and build good will on those separate tracks. Engaging with China has value, even if it offers no near-term possibility for agreement on some strategic issues.[111] Regular government to government dialogs have value in keeping the diplomatic door open. This does not mean a posture that is any less aggressive on the policies that matter most. The U.S. can continue to implement policies that pressure China on other, more difficult issues, and deliver consistent messaging on what changes the U.S. wants to see in China's policies.

Uniting Tech Democracies: The T-10

The most critical element in addressing the China challenge is building a coalition of like-minded technology democracies to advance more open and democratic values in technology policy, while countering China's harmful approaches to technology and data governance.

This small group of liberal democracies with advanced technology sectors would include 10-12 countries. In their recent Foreign Affairs piece on the subject, Jared Cohen and Richard Fontaine argue for including the U.S., France, Germany, Japan, and the United Kingdom, which all have large economies and innovative technology sectors, Australia, Canada, and South Korea, which have smaller economies but are also important players in technology, and Finland and Sweden, which are telecommunications and engineering powerhouses.[112] Some have also advocated for including India and Israel, owing to the global reach of their flourishing technology and startup sectors. Both the U.K. and the EU have recently made similar calls for an alliance of tech-democracies to align tech policies and coordinate approaches vis-a-vis China.[113]

The agenda of such a "T-10" alliance could be quite broad, including agreement on issues such as data privacy and digital tax, government access to

data, as well as trade issues, including enabling cross border data flows and limiting server localization requirements. It should also include efforts to safeguard citizens from harmful and illegal content online. Most importantly, the tech democracy alliance should advance a vision and system of governance for the global digital ecosystem that is open, accountable, and democratic.

The tech democracy alliance should advance a vision and system of governance for the global digital ecosystem that is open, accountable, and democratic.

The tech-democracies should look to align policies and collaborate across a wide range of areas, both those that seek to protect key technologies or challenge China's unfair practices, as well as those that bolster key technologies. For this effort to have a meaningful chance to succeed, the U.S. and Europe must make progress on overcoming divisions on key technology policy issues such as privacy, competition, and tax (see more below). Japan can play a crucial bridging function, given its strong relations with the U.S. and adequacy determination from the EU. Together, the U.S., EU, and Japan, can form the core of the new alliance.

This new global governance framework will allow businesses, citizens and civil society access to an internet that is open, democratic, and safe. It will also form a template for expanding these concepts through negotiating digital agreements with other countries, understanding that other countries may need to phase in or adapt parts of the agenda.

Export Controls

As mentioned in the Invest in America section of this paper, in 1996, a group of 42 countries agreed to a voluntary arrangement to control exports and transfers of goods on an agreed upon list of sensitive technologies, called the Wassenaar Arrangement. The process of updating the products and technologies on this list has proven to be lengthy and cumbersome, leading the U.S. to impose unilateral export controls on certain technologies, forbidding their export to China. These recent controls have not been coordinated with allies, eroding their effectiveness. In addition to coordinating through

Wassenaar on future controls, the T-10 should identify technologies of key concern and coordinate on a nimbler set of controls for those technologies.

Supply Chain Measures

The Trump Administration had legitimate concerns regarding the security risks of using Huawei network technology, however its approach of strong-arming other nations to eliminate Huawei from their networks, while mostly successful, was not ideal. The T-10 should work together to develop a common set of principles for building out 5G networks and ensuring that countries have access to safe and secure equipment in their networks. Such an approach could be expanded to include supply chains for other important technologies and build on the Prague Proposals, a security framework for 5G networks.[114]

Cybersecurity

Cybersecurity is a massive global problem with economic, security and human rights implications. The 2017 WannaCry ransomware attack infected hundreds of thousands of computer networks in 150 countries, with losses totaling up to $4 billion.[115] According to the U.S. Council of Economic Advisers, malicious cyber activity caused between $56 billion and $109 billion in damage to the U.S. economy in 2016 alone.[116] More recently, the hacking of numerous government agencies in December 2020, thought to be engineered by Russia, could have far reaching national security implications.[117] While the United Nations and other groups have launched international efforts to coordinate cybersecurity norms and regulations, these large initiatives have had limited success due to differences in goals and levels of transparency among nations. The T-10 could lead by developing agreement around cybersecurity norms and incentives to encourage adoption of those norms.

Coordinated Trade Actions

China has long subsidized its companies and especially its technology companies. As the Center for American Progress and others have noted, China provides a wide array of direct and indirect subsidies that reduce Huawei's operational costs, speed time to market for its products, and allow it to price

its products well below prices set by competitors.[118] Chinese state banks also provide generous financing to Huawei's customers on terms most commercial banks cannot match. While Huawei is the most obvious example of this strategy, China uses these practices broadly with many of its technology companies.

The World Trade Organization's (WTO) Agreement on Subsidies and Countervailing Measures (ASCM) is out of date and did not contemplate many of the subsidies currently employed by China. Efforts by the U.S., the EU, and Japan to reform the WTO rules governing industrial subsidies and state-owned enterprises led to progress in January 2020, and should be continued. The trilateral group agreed that the list of subsidies prohibited under the ASCM should be expanded and proposed changes to make it easier to impose countervailing duties on actionable subsidies.[119] The T-10 should collaborate on this effort to impose disciplines on China's subsidies.

The T-10 should also work together to investigate below-market-rate loans by the China Development Bank and consider filing a joint WTO case against these below market financing measures.

Standards Setting

China has allocated significant resources toward the hundreds of international standards setting organizations and is in leadership positions in many of these groups, allowing it to advocate for global adoption of Chinese standards. Melanie Hart, previously with the Center for American Progress, notes that U.S. private sector participants in standards bodies may represent their own companies' interests, while the Chinese government requires Chinese firms to vote as a bloc to support China's proposals and to support Chinese nationals for leadership roles in standards bodies.[120]

Adoption of Chinese standards by these bodies facilitates sales of Chinese products and could have troubling implications for human rights and democracy. Standards recently advocated by China would encourage top-down internet control, which Lindsey Gorman of the German Marshall Fund pointed out could be used to silence journalists or activists who run afoul of the government.[121] The U.S. should work with other tech democracies to assert

greater leadership in international standards setting bodies and ensure fair and transparent processes in those organizations. The T-10 needs to take the lead on setting standards for new technologies, like IoT, AI, and apps, to ensure that shared values of democracy and openness are infused in the outcomes of standards setting for internet and information technologies.

Joint Research & Development

While China's share of global R&D spending is rising, Georgetown's Center for Security and Emerging Technology (CSET) notes that the U.S. and its allies together still comprise a majority of global R&D. Given this fact, to compete with China, CSET asserts that America's future lies in technical alliances. Similarly, the Harvard Belfer Center recommends that "deepened U.S.-EU cooperation across the entire AI ecosystem is necessary to advance a more secure, safe, and prosperous world."[122] Working together on a humancentric approach, focusing on technology's impact on people and human rights, and dealing with issues such as facial recognition will be key.

While countries in the T-10 compete in many areas of technology development, the alliance could agree on joint R&D projects in a few key strategic areas, such as 5G and its successors, where China's subsidies make it difficult for others to enter the market. As Cohen and Fontaine point out, joint funds could be used to support non-Chinese 5G companies as they transition to a next generation open radio access network (ORAN) system.[123]

Financing

There are several measures the T-10 countries could use to counter China's subsidization of its exports. First, the T-10 countries should work together to encourage China to adopt the OECD Export Credit Arrangement, a framework for the orderly use of officially supported export credits to encourage competition among exporters based on quality and prices of goods and services exported, rather than on the most favorable officially supported export credits.[124] The OECD arrangement limits financing terms and conditions (repayment terms, minimum premium rates, minimum interest rates) to be applied when providing officially supported export credits, as well as on the

use of tied aid by the participants.[125] The Arrangement also contains various transparency provisions. These provisions would help to ensure China's Belt-and-Road Initiative and China Development Bank loans are financed based on market principles and not just subsidies to Chinese exporters.

Secondly, the T-10 should explore joint financing for technology exports. The Competitiveness section of this paper discussed the concept of a Digital Marshall Fund – a fund dedicated to providing competitive export financing for U.S. technology firms competing with Huawei or other Chinese companies offering subsidized financing. The T-10 could explore collaborating on such a fund and use it to support technology companies competing with Chinese companies using subsidized financing, as well as to support Nokia and Ericsson, which currently provide the only 5G alternatives to Huawei. Such a fund would provide developing countries that want to purchase trusted 5G or other technologies that promote open and democratic values an affordable alternative to Chinese technology.

Establishing Broader Digital Governance and Trade Arrangements

Beyond the T-10, there are important opportunities for broader digital alliances and agreements. While not as comprehensive as the T-10, these alliances and agreements would serve an important role in codifying rules for digital governance and trade with a broader range of countries. No global rules govern digital trade, which covers everything from e-commerce to bank transfers to telemedicine. Global e-commerce sales alone topped $3.5 trillion in 2019.[126] Covid-19 has only accelerated e-commerce growth and the importance of the digital economy as services like tele-health and education are increasingly moving across traditional borders, increasing the need for all countries to have access to an internet that is open, accountable, and democratic.

In 2019, 76 countries in the WTO formally launched negotiations on an e-commerce agreement.[127] However, given the large number of countries

involved, including Russia, China and others who have different approaches to key issues, these negotiations are moving slowly and may result in little action or an agreement with a low level of ambition.

Several regional agreements incorporating higher standards for compliance have provisions that lay the groundwork for a broader digital agreement. The USMCA, for example, made progress developing rules for digital trade and governance,[128] and was one of the first trade agreements to include provisions on cybersecurity. The digital trade rules in USMCA provide a clear, simple bar to data localization; clarify circumstances in which privacy and data protection exceptions can be made; recognize the APEC CBPR as a valid system for data transfers; and include commitments on cybersecurity. The agreement also provides that parties will consider creating a forum to promote cooperation on digital trade issues, including those related to cybersecurity. Like approaches reflected in the USMCA, the U.S.-Japan Digital Trade Agreement provides a baseline from which to work and represents a "comprehensive and high standard."

Several other countries have negotiated agreements that provide ideas on which to build. Singapore, New Zealand, and Chile have finalized an open plurilateral agreement, the Digital Economy Partnership Agreement (DEPA), which includes provisions governing digital identities, data flow, and AI. The agreement will enter into force when at least two of the parties have completed the domestic legal processes required, as it did for New Zealand and Singapore on January 7, 2021,[129] and it is open to other WTO members to join. DEPA is novel in that it allows countries to join certain modules, rather than requiring adoption of the full agreement.[130]

Singapore and Australia also concluded a bilateral digital agreement in March 2020, and Singapore and South Korea recently launched negotiations on a digital agreement. These agreements go beyond the digital rules in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and include provisions for nondiscriminatory treatment of electronic transactions and other consumer protections.

Capacity exists to go further toward establishing rules that foster trust in and responsible use of technology and enable more people in the U.S. and worldwide to enjoy its benefits. Negotiating agreements with a larger number of countries is important to gain broader consensus regarding digital governance, facilitate the flow of data across borders, develop global digital standards, and encourage regulatory cooperation.[131]

Given DEPA, USMCA, and the other digital deals in the region, along with CPTPP, the time is ripe for the U.S. to pursue a Pacific digital agreement to set high standards and rebuild trust in the region. This initiative would build on momentum in the Asia-Pacific region, counter trends toward a more fragmented approach to digital trade, and ensure that these countries enact a democratic internet governance agenda.

No.	Digital Trade Provisions	USMCA	CPTPP	A-HKFTA	SLSFTA	KORUS FTA	EUJEPA	EUSFTA
1	Elimination of customs duties on digital products and/or electronic transmissions	YES	YES	YES	YES	YES	YES	YES
2	Non-discrimination against digital products	YES	YES	NO	YES	YES	NO	NO
3	Electronic authentication and electronic signatures	YES	YES	YES	YES	YES	YES	PARTIAL
4	Paperless trading	YES	YES	YES	YES	YES	NO	PARTIAL
5	Domestic electronic transactions framework	YES	YES	YES	YES	YES	PARTIAL	NO
6	Online consumer protection	YES	YES	YES	YES	YES	YES	NO
7	Personal information protection	YES	YES	YES	YES	NO	NO	NO
8	Measures agains unsolicited commercial electronic communications	YES	YES	YES	NO	NO	YES	NO
9	Cybersecurity	YES	YES	NOA	NO	NO	NO	NO
10	Cross-border transfer of information	YES	YES	YES	YES	PARTIAL	YES	YES
11	Prohibition of data localisation	YES	YES	YES	YES	NO	NO	NO
12	Cross-border transfer of information by electronic means and prohibition of data localisation for financial services	NO	NO	NO	NO	PARTIAL	NO	NO
13	Liability of intermediary service providers	YES	NO	NO	NO	NO	NO	PARTIAL
14	Non-disclosure of software source code and related algorithms	YES	PARTIAL	PARTIAL	NO	NO	PARTIAL	NO
15	Open government data	YES	NO	NO	NO	NO	NO	NO
16	Cooperation	YES	YES	YES	YES	YES	YES	YES

Source: http://asiantradecentre.org/talkingtrade/comparing-digital-rules-in-trade-agreements

Building bridges toward the EU will also be critical in creating an environment for the healthy development of digital trade. If the U.S. and EU can bridge their divides, they can form the core of a global alliance of countries whose

approach to technology is grounded in openness and respect for privacy and other fundamental rights. Such an agreement could be reached in the context of larger U.S.-EU negotiations, or as a foundation for the T-10 Alliance described above.

A Pacific Digital Agreement would be another prong in the broader effort to build a system of global digital governance. Such an agreement will also be important in reasserting U.S. engagement and leadership in Asia, a region that sorely missed U.S. engagement during the Trump Administration. An alliance of techno-democracies (T-10) followed by a Pacific Digital Agreement will go a long way to setting global digital governance norms and are key pieces of a U.S. strategy to bolster digital leadership.

Reaching Agreement on Global Digital Tax Issues

With global digital trade increasing exponentially, countries have become increasingly interested in taxing that trade to generate revenue. This interest has become more urgent with Covid-19, as federal coffers are over-stretched and countries are looking for new ways to raise funds. Digital taxation has been a contentious issue in recent years, with deep divisions between the U.S., which would generally like to avoid taxes on digital companies, since many of the largest digital companies are American, and the EU and other countries, including Brazil and India, which would like to tax those companies to bring in more revenue. Many in the U.S. recognize that international tax rules need to be updated to address widespread digitalization and the changes it has created. And the widespread use of remote work brought on by Covid-19 will lead to further changes to our thinking about the location of economic activity and how it should be taxed.

In 2019, the U.S. launched a Section 301 investigation into France's digital service tax (DST), arguing that the tax, which would only impact companies earning over 750 million euros globally, would primarily affect U.S. firms, and would therefore be de facto discriminatory.[132]

The OECD issued a report in 2019 suggesting an approach to develop a framework for digital taxation, along with some broader related tax issues like Base Erosion and Profit Shifting (BEPS). Negotiations are proceeding and there was hope that an agreement could be reached in 2020, but divisions among the parties have, to date, precluded an agreement.

In early June 2020, the U.S. voiced frustration that countries were continuing to propose or impose DSTs while the negotiations were in progress. In response, it launched Section 301 investigations against nine countries plus the EU,[133] and later the same month announced that it was pulling out of the OECD negotiations.[134] With talks at a stalemate, countries moving forward to impose DSTs, and the U.S. threatening to impose tariffs in retaliation, the risk of a trade war is significant.

The U.S. should rejoin the OECD talks, both to resolve this issue and as a show of good faith to its allies. Early indications on this from the new Biden Administration are encouraging. We must prioritize negotiating an agreement governing DSTs that will facilitate as well as minimize friction in global digital trade. The U.S. may eventually have to accept some level of tax on its companies' e-commerce activities as a trade-off for avoiding even higher taxes in many countries, and to minimize compliance challenges due to different DSTs across the globe.

Leading Globally Summary of Recommendations:

Tech-Democracies

- The U.S. should build a coalition of like-minded technology democracies (T-10) to develop a high standard digital governance agenda advancing open and democratic values to counter China's autocratic approaches to technology and data governance.
- The T-10 should coordinate efforts in a variety of areas, including privacy, export controls, supply chain measures, cybersecurity, network and data

security, online safety, and technology standards. As a point of departure for this effort, the U.S. and Europe must reduce current divisions over technology policy and strengthen cooperation with Japan.

- The T-10 should pursue coordinated trade actions, including increasing disciplines against subsidies in the WTO to address China's practices, explore filing a joint WTO case against China Development Bank loans, and encourage China to join the OECD Export Credit Arrangement.
- Finally, the T-10 should consider pursuing joint R&D in key technology sectors, as well as joint financing to allow companies in member countries to compete with Chinese companies on a level playing field.

Pacific Digital Agreement

- The U.S. should negotiate an Asia-Pacific Digital Agreement that embodies the values of democracy and openness, using existing regional building blocks, like key provisions in USMCA, the U.S.-Japan Digital Trade Agreement, the DEPA Agreement between Singapore, New Zealand and Chile, and CPTPP. Such an agreement will also play an important role in reestablishing U.S. engagement in Asia.

Digital Tax

- The U.S. should rejoin the OECD talks and prioritize negotiating an agreement governing digital service taxes which will be key to eliminating a rift with EU allies, laying the groundwork for the broader T-10 digital governance agenda. The U.S. may have to accept some level of taxation as part of that compromise.

Conclusion:

The digital future is already here, dramatically accelerated by a pandemic that has changed how the world works, learns, and plays – trends that will escalate in the years to come. Now is the time for the U.S. to launch a comprehensive global digital strategy. The risks of not seizing this opportunity are immense, posing existential risks to the U.S. economy and global democracy. The Biden Administration must seize this moment to launch a comprehensive, whole of government, digital strategy, providing good jobs for workers sidelined by automation and upgrading U.S. competitiveness, positioning the U.S. to become a global digital leader. The Administration must also work with its allies to develop a digital governance structure and jointly pursue policies to meet the China challenge.

The digital revolution is at an inflection point – with the right policies and investments, the new Administration can create a better future for its citizens and forge a new era of U.S. global leadership based on shared democratic values.

Endnotes

1 Monica Anderson and Madhumitha Kumar, "Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption," Pew Research Center, May 7, 2019, https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/

2 Ibid.

3 Brookings, "Nearly Every Job is Becoming More Digital – Brookings Study," November 15, 2017, https://www.kurzweilai.net/nearly-every-job-is-becoming-more-digital-brookings-study; Mark Muro, Sifan Liu, Jacob Whiton, and Siddharth Kulkarni, "Digitalization and the American Workforce," Metropolitan Policy Program at Brookings, November 2017, https://www.brookings.edu/research/digitalization-and-the-american-workforce/

4 Edward Alden and Laura Taylor-Kale, "The Work Ahead: Machines, Skills, and U.S. Leadership in the Twenty-First Century," Independent Task Force Report No. 76, Council on Foreign Relations, April 2018, https://www.cfr.org/report/the-work-ahead/report/

5 Muro, Liu, Whiton, and Kulkarni, "Digitalization and the American Workforce," https://www.brookings.edu/research/digitalization-and-the-american-workforce/

6 Derek Thompson, "Denmark's Unemployment Benefits System, and Ours," *The Atlantic,* August 17, 2010, https://www.theatlantic.com/business/archive/2010/08/denmarks-unemployment-benefits-system-and-ours/61615/

7 "My Skills Future," https://www.myskillsfuture.sg/content/portal/en/index.html

8 Tamar Jacoby, "Why Germany is So Much Better at Training Its Workers," *The Atlantic,* October 16, 2014, https://www.theatlantic.com/business/archive/2014/10/why-germany-is-so-much-better-at-training-its-workers/381550/

9 Sally Weale, "Lessons from Estonia: Why It Excels at Digital Learning During Covid," *The Guardian,* October 30, 2020, https://www.theguardian.com/world/2020/oct/30/lessons-from-estonia-why-excels-digital-learning-during-covid

10 Sarah Butrymowicz, "Is Estonia the New Finland," *The Atlantic,* June 23, 2016, https://www.theatlantic.com/education/archive/2016/06/is-estonia-the-new-finland/488351/

11 "Public Spending on Labour Markets," OECD, https://data.oecd.org/socialexp/public-spending-on-labour-markets.htm

12 "Toward a New Capitalism," The Aspen Institute Future of Work Initiative, 2016, https://www.aspeninstitute.org/wp-content/uploads/2017/01/New_Capitalism_Narrative.pdf

13 "Job Openings and Labor Turnover Summary," U.S. Bureau of Labor Statistics, January 12, 2021, https://www.bls.gov/news.release/jolts.nr0.htm

14 "Digital Skills Gap Narrows But Still Persists from Classroom to Boardroom – Deloitte," Deloitte, January 9, 2019, https://www2.deloitte.com/uk/en/pages/press-releases/articles/digital-skills-gap-narrows-but-still-persists-from-classroom-to-boardroom.html

15 Alden and Taylor-Kale, "The Work Ahead," https://static-live-backend.cfr.org/report/the-work-ahead/report/findings.php

16 Erin Duffin, "Community Colleges in the United States - Statistics & Facts," Statista, February 6, 2020, https://www.statista.com/topics/3468/community-colleges-in-the-united-states/

17 "FACT SHEET - White House Unveils America's College Promise Proposal: Tuition-Free Community College for Responsible Students," The White House, January 9, 2015,

https://obamawhitehouse.archives.gov/the-press-office/2015/01/09/fact-sheet-white-house-unveils-america-s-college-promise-proposal-tuitio

18 Robert Lerhman, "Expanding Apprenticeship Opportunities in the United States," Brookings, June 19, 2014, https://www.brookings.edu/research/expanding-apprenticeship-opportunities-in-the-united-states/

19 Apprenticeship Carolina SC Technical College System, http://www.apprenticeshipcarolina.com/about.html

20 "Apprenticeship System in Germany," Apprenticeship Toolbox, https://www.apprenticeship-toolbox.eu/germany/apprenticeship-system-in-germany/143-apprenticeship-system-in-germany

21 Isobel Leybold-Johnson, "Why the World Should Take Note of the Swiss Apprenticeship Model," SWI, March 10, 2020, https://www.swissinfo.ch/eng/why-the-world-should-take-note-of-the-swiss-apprenticeship-model/45810312

22 "Registered Apprenticeship: Federal Role and Recent Federal Efforts," CRS Report No. R45171, Congressional Research Service, September 25, 2019, https://crsreports.congress.gov/product/pdf/R/R45171

23 "History and Fitzgerald Act," U.S. Department of Labor Employment and Training Administration, https://www.dol.gov/agencies/eta/apprenticeship/policy/national-apprenticeship-act

24 Angela Hanks and Ethan Gurwitz, "How States are Expanding Apprenticeship," Center for American Progress, February 9, 2016, https://www.americanprogress.org/issues/economy/reports/2016/02/09/130750/how-states-are-expanding-apprenticeship/

25 Angela Hanks, "The Administration and Congress Should Not Undermine Registered Apprenticeships," Center for American Progress, January 11, 2018, https://www.americanprogress.org/issues/education-postsecondary/reports/2018/01/11/444829/administration-congress-not-undermine-registered-apprenticeships/

26 "Registered Apprenticeship National Results Fiscal Year 2019," U.S. Department of Labor Employment and Training Administration, https://www.dol.gov/agencies/eta/apprenticeship/about/statistics

27 Angela Hanks, Annie McGrew, and Daniella Zessoules, "The Apprenticeship Wage and Participation Gap," Center for American Progress, July 11, 2018, https://www.americanprogress.org/issues/economy/reports/2018/07/11/453321/apprenticeship-wage-participation-gap/

28 Agam Shah, "Seeking Tech Talent, Companies Kickstart Apprenticeship Programs, *The Wall Street Journal,* January 30, 2020, https://www.wsj.com/articles/seeking-tech-talent-companies-kickstart-apprenticeship-programs-11580396400

29 Senator Chris Coons, "Sens. Coons, Young, Reps. Norcross, McKinley Bill to Expand Registered Apprenticeships in High-Growth Job Sectors Passes House," December 2, 2020, https://www.coons.senate.gov/news/press-releases/sens-coons-young-reps-norcross-mckinley-bill-to-expand-registered-apprenticeships-in-high-growth-job-sectors-passes-house

30 Peter Boyland, "The State of the Mobile Network Experience," Opensignal, May 2019, https://www.opensignal.com/sites/opensignal-com/files/data/reports/global/data-2019-05/the_state_of_mobile_experience_may_2019_0.pdf

31 "Internet/Broadband Fact Sheet," Pew Research Center, June 12, 2019, https://www.pewresearch.org/internet/fact-sheet/internet-broadband/#who-has-home-broadband

32 Anderson and Kumar, "Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption," https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/

33 Ibid.

34 "Millions of Kids Are Struggling in School Because They Don't Have Internet Access at Home," *Associated Press,* June 10, 2019, https://www.marketwatch.com/story/nearly-3-million-students-in-the-us-struggle-to-keep-up-in-school-due-to-lack-of-home-internet-2019-06-10

35 Jamari Simama, "It's 2020. Why Is the Digital Divide Still With Us?" *Governing,* March 5, 2020, https://www.governing.com/now/Its-2020-Why-Is-the-Digital-Divide-Still-with-Us.html

36 Klint Finley, "When School Is Online, the Digital Divide Grows Greater," *Wired,* April 9, 2020, https://www.wired.com/story/school-online-digital-divide-grows-greater/

37 Meagan Flynn, "Teleworking in a Parking Lot. School on a Flash Drive. The Coronavirus Prompts New Urgency for Rural Internet Access." *Washington Post,* October 14, 2020, https://www.washingtonpost.com/local/va-politics/rural-broadband-virginia/2020/10/14/bdcc9a4c-0a5b-11eb-859b-f9c27abe638d_story.html

38 "Bridging Rural America to the Future of Work," Center on Rural Innovation, https://ruralinnovation.us/our-work/#broadband

39 "Wicker, Capito, Blackburn Introduce Bill to Accelerate Deployment of Rural Digital Opportunity Fund Broadband Networks," U.S. Senate Committee on Commerce, Science, & Transportation, June 22,2020, https://www.commerce.senate.gov/2020/6/wicker-capito-blackburn-introduce-bill-to-accelerate-deployment-of-rural-digital-opportunity-fund-broadband-networks

40 Senator Amy Klobuchar, "Klobuchar, Clyburn Introduce Comprehensive Broadband Infrastructure Legislation to Expand Access to Affordable High-Speed Internet," July 1, 2020, https://www.klobuchar.senate.gov/public/index.cfm/2020/7/klobuchar-clyburn-introduce-comprehensive-broadband-infrastructure-legislation-to-expand-access-to-affordable-high-speed-internet

41 Carl Weinschenk, "OpenVault: Pandemic Drives Almost a Year's Worth of Broadband Traffic Growth in the Span of a Couple of Weeks," May 4, 2020, *Telecompetitor,* https://www.telecompetitor.com/openvault-pandemic-drives-almost-a-years-worth-of-broadband-traffic-growth-in-the-span-of-a-couple-of-weeks/

42 Charles Cooper, "Spectrum Sharing: An Emerging Success," National Telecommunications and Information Administration, August 19, 2020, https://www.ntia.gov/blog/2020/spectrum-sharing-emerging-success

43 Competitive Carriers Association, "Spectrum: The Lifebook of the Wireless Industry," https://www.ccamobile.org/advocacy#Spectrum

44 CTIA, "Spectrum Policy," https://www.ctia.org/positions/spectrum

45 Sascha Meinrath and Nathalia Foditsch, "How Other Countries Deal with Net Neutrality," *Smithsonian Magazine,* December 15, 2017, https://www.smithsonianmag.com/innovation/how-other-countries-deal-net-neutrality-180967558/

46 Klint Finely, "The WIRED Guide to Net Neutrality," *Wired,* May 5, 2020, https://www.wired.com/story/guide-net-neutrality/

47 Sara Morrison, "How Biden's FCC Could Fix America's Internet," *Vox Recode,* January

21, 2021, https://www.vox.com/recode/21557495/biden-fcc-digital-divide-net-neutrality-section-230

48 Klint Finley, "Washington State Enacts Net Neutrality Law, in Clash with FCC," *Wired,* March 5, 2018, https://www.wired.com/story/washington-state-enacts-net-neutrality-law-in-clash-with-fcc/

49 Klint Finley, "California Net Neutrality Bill Would Go Beyond Original Protections," *Wired,* March 14, 2018, https://www.wired.com/story/california-net-neutrality-bill-would-go-beyond-original-protections/

50 Agam Shah, "10 Arguments For and Against Net Neutrality, Part 1," American Society of Mechanical Engineers, March 22, 2018, https://www.asme.org/topics-resources/content/10-arguments-against-net-neutrality-part-1

51 "Net Neutrality Letter from Mayor Walsh, Other Local Leaders," City of Boston, December 7, 2017, https://www.boston.gov/news/net-neutrality-letter-mayor-walsh-other-local-leaders

52 "Internet Privacy Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility," Report to the Chairman, Committee on Energy and Commerce, House of Representatives, Report GAO-19-52, U.S. Government Accountability Office, January 2019, https://www.gao.gov/assets/700/696437.pdf

53 Orson Lucas and Steven Stein, "The new imperative for corporate data responsibility," KPMG, 2020, https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf

54 Julie Brill, "Revisiting the Need for Federal Data Privacy Legislation," Written Testimony Before the U.S. Senate Committee on Commerce, Science, & Transportation, September 23, 2020, https://www.commerce.senate.gov/services/files/5404DCED-136B-4622-B922-49045EC7C03E

55 "The OECD Privacy Framework," OECD, 2013, http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

56 "Data Flows, Online Privacy, and Trade Policy," CRS Report R45584, Congressional Research Service, March 11, 2019, https://fas.org/sgp/crs/row/R45584.pdf

57 Scott Kennedy, "Made in China 2025," Center for Strategic and International Studies, June 1, 2015, https://www.csis.org/analysis/made-china-2025

58 Adam Segal, "Innovation and National Security: Keeping Our Edge," Independent Task Force Report No. 77, Council on Foreign Relations, September 2019, https://www.cfr.org/report/keeping-our-edge/findings/#_edn61

59 "Is China a Global Leader in Research and Development?" China Power, August 25, 2020, https://chinapower.csis.org/china-research-and-development-rnd/

60 Caleb Foote and Rob Atkinson, "Federal Support for R&D Continues Its Ignominious Slide," Information Technology & Innovation Foundation, August 12, 2019, https://itif.org/publications/2019/08/12/federal-support-rd-continues-its-ignominious-slide#:~:text=Indeed%2C%20in%2022%20of%20the%2028%20years%20following,the%20latest%20data%20from%20the%20National%20Science%20Foundation

61 Abby Joseph Cohen and Michael Hao Wu, "The Coronavirus Pandemic and U.S. Federal Investment in Science," Goldman Sachs, April 29, 2020, https://www.gspublishing.com/content/research/en/reports/2020/04/29/67c9cada-68a2-48af-b25c-0f5416c-0c0c8.html

62 Derek Johnson, "Can the U.S. Compete in R&D?" *Federal Computer Week,* January 30, 2020, https://fcw.com/articles/2020/01/30/research-spending-us-china-congress.aspx

63 James Pethokoukis, "U.S. Federal Research Spending Is at a 60-year Low. Should We Be Concerned?" American Enterprise Institute, May 11, 2020, https://www.aei.org/economics/us-federal-research-spending-is-at-a-60-year-low-should-we-be-concerned/, Matthew P. Goodman and Dylan Gerstel, "Sharpening America's Innovative Edge, Center for Strategic and International Studies, October 16, 2020, https://www.csis.org/analysis/sharpening-americas-innovative-edge

64 Senator Todd Young, "Young, Schumer Unveil Endless Frontier Act to Bolster U.S. Tech Leadership and Combat China," May 27, 2020, https://www.young.senate.gov/newsroom/press-releases/young-schumer-unveil-endless-frontier-act-to-bolster-us-tech-leadership-and-combat-china

65 Scott Kennedy, "Washington's China Policy Has Lost Its Wei," Center for Strategic and International Studies, July 27, 2020, https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei

66 Stuart Anderson, "Immigrants and Billion Dollar Startups," NFAP Policy Brief, National Foundation for American Policy, March 2016, https://nfap.com/wp-content/uploads/2016/03/Immigrants-and-Billion-Dollar-Startups.NFAP-Policy-Brief.March-2016.pdf

67 Daniel Kim, "Getting the Job Done: How Immigrants Expand the U.S. Economy," University of Pennsylvania Wharton, September 8, 2020, https://knowledge.wharton.upenn.edu/article/how-immigrants-expand-the-u-s-economy/

68 Abby Joseph Cohen and Michael Hao Wu, "Immigration and the U.S. Workforce," Goldman Sachs, August 13, 2019, https://www.goldmansachs.com/insights/pages/gs-research/immigration-and-the-us-workforce/report.pdf

69 Segal, "Innovation and National Security: Keeping Our Edge," https://www.cfr.org/report/keeping-our-edge/findings/#_edn33

70 Ted Hesson, "Trump Officials Rush to Make It Tougher for Skilled Foreign Workers to Gain Visas," *Reuters,* September 21, 2020, https://www.reuters.com/article/usa-election-immigration-workers/trump-officials-rush-to-make-it-tougher-for-skilled-foreign-workers-to-gain-visas-idUSKCN26C2T4

71 Britta Glennon, "How Do Restrictions on High-Skilled Immigration Affect Offshoring? Evidence from the H-1B Program," Working Paper 27538, National Bureau of Economic Research, http://www.nber.org/papers/w27538

72 "Fairness for High-Skilled Immigrants Act of 2020 (S.386), AILA Doc. No. 20120333, American Immigration Lawyers Association, https://www.aila.org/advo-media/issues/all/featured-issue-legislation-impacting-per-country/latest-text-of-the-fairness-for-high-skilled

73 Jason Oxman, Letter to President Trump, Information Technology Industry Council, June 9, 2020, https://www.itic.org/dotAsset/a2cb846e-459f-4b8c-b792-a5881b-37c8ab.pdf

74 "Entity List," U.S. Department of Commerce Bureau of Industry and Security, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list; "Commerce Department Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List," U.S. Department of Commerce Bureau of Industry and Security,

U.S. Department of Commerce, May 15, 2019, https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd; "Department of Commerce Adds Dozens of New Huawei Affiliates to the Entity List and Maintains Narrow Exemptions through the Temporary General License," U.S. Department of Commerce, August 19, 2019, https://www.commerce.gov/news/press-releases/2019/08/department-commerce-adds-dozens-new-huawei-affiliates-entity-list-and

75 Chad Bown, "How Trump's Export Curbs on Semiconductors and Equipment Hurt the U.S. Technology Sector," Peterson Institute for International Economics, September 28, 2020, https://www.piie.com/blogs/trade-and-investment-policy-watch/how-trumps-export-curbs-semiconductors-and-equipment-hurt-us

76 "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies," U.S. Department of Commerce, May 15, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts; "Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List," U.S. Department of Commerce, August 17, 2020, https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and

77 Kevin Wolf, "Export Controls Will Become More Effective When They Include Plurilateral Controls," Center for a New American Security, August 13, 2020, https://www.cnas.org/publications/commentary/export-controls-will-become-more-effective-when-they-include-plurilateral-controls

78 Bown, "How Trump's Export Curbs on Semiconductors and Equipment Hurt the U.S. Technology Sector," https://www.piie.com/blogs/trade-and-investment-policy-watch/how-trumps-export-curbs-semiconductors-and-equipment-hurt-us

79 Paul Marquardt, Chase D. Kaniecki, Nathanael Kurcab, "BIS Issues Long-Awaited Request for Public Comment on Foundational Technologies," Cleary Gottlieb, August 31, 2020, https://www.clearytradewatch.com/2020/08/bis-issues-long-awaited-request-for-public-comment-on-foundational-technologies/#_ftn4

80 "Identification and Review of Controls for Certain Foundational Technologies," Federal Register 85 FR 52934, U.S. Department of Commerce Bureau of Industry and Security, August 27, 2020, https://www.federalregister.gov/documents/2020/08/27/2020-18910/identification-and-review-of-controls-for-certain-foundational-technologies

81 Wolf, "Export Controls Will Become More Effective When They Include Plurilateral Controls," https://www.cnas.org/publications/commentary/export-controls-will-become-more-effective-when-they-include-plurilateral-controls

82 "Summary of the Foreign Investment Risk Review Modernization Act of 2018," U.S. Department of Treasury, https://home.treasury.gov/system/files/206/Summary-of-FIRRMA.pdf

83 "Timeline of Federal U.S. Actions on Tech Supply Chain Risk Management," Information Technology Industry Council, accessed January 2021, https://www.itic.org/policy/ITI-SupplyChainRiskManagementGraphic.pdf

84 "Commerce Department Issues Interim Rule to Secure the ICTS Supply Chain," U.S. Department of Commerce, January 14, 2021, https://www.commerce.gov/news/press-releases/2021/01/commerce-department-issues-interim-rule-secure-icts-supply-chain

85 Stephen Ezell, "Digital Trade Growth, Rule-Making, and Supply Chain Resiliency: U.S. and Global Perspectives," Information Technology Industry Council, October 26, 2020, http://www2.itif.org/2020-ezell-digital-trade-growth.pdf?_ga=2.246635143.2057729694.1606146603-656988604.1606146603

86 Colin Black Andrews and Patrick Lozada, "Comments of the Telecommunications Industry Association," In the Matter of the National Strategy to Secure 5G Implementation Plan, Docket No. 200521-0144, Telecommunications Industry Association, June 25, 2020, https://www.ntia.doc.gov/files/ntia/publications/tia-06252020.pdf

87 Magdalena Petrova, "We Traced What It Takes to Make an iPhone From Its Initial Design to the Components and Raw Materials Needed to Make It a Reality," *CNBC,* December 14, 2018, https://www.cnbc.com/2018/12/13/inside-apple-iphone-where-parts-and-materials-come-from.html

88 Miyeon Oh, Robert Dohner, and Trey Herr, "Global Value Chains in an Era of Strategic Uncertainty: Prospects for US-ROK Cooperation," *The Atlantic Council,* November 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/11/global-value-chains-final-11-19-1.pdf

89 Representative Michael McCaul, "China Task Force Report," 116th U.S. Congress, September 2020, https://gop-foreignaffairs.house.gov/wp-content/uploads/2020/09/china-task-force-report-final-9.30.20.pdf

90 Jack Corrigan, "CIA, NSA Offer Startups More Than Money," *Nextgov,* November 2, 2017, https://www.nextgov.com/emerging-tech/2017/11/cia-nsa-offer-startups-more-money/142257/

91 Stephen Ezell and Scott Andes, "Localizing the Economic Impact of Research and Development: Policy Proposals for the Trump Administration and Congress," Information Technology and Innovation Foundation, December 7, 2016, https://itif.org/publications/2016/12/07/localizing-economic-impact-research-and-development-policy-proposals-trump

92 Sen. Amy Klobuchar, "Klobuchar, Coons, Kaine, King Introduce Legislation to Protect and Strengthen Young Businesses Across the Country, March 19, 2020, https://www.klobuchar.senate.gov/public/index.cfm/2020/3/klobuchar-coons-kaine-king-introduce-legislation-to-protect-and-strengthen-young-businesses-across-the-country

93 Bianca Majumder, "Congress Should Revive the Office of Technology Assessment," Center for American Progress, May 13, 2019, https://www.americanprogress.org/issues/green/news/2019/05/13/469793/congress-revive-office-technology-assessment/

94 Lee Drutman and Steven M. Teles, "Why Congress Relies on Lobbyists Instead of Thinking for Itself," *The Atlantic,* March 10, 2015, https://www.theatlantic.com/politics/archive/2015/03/when-congress-cant-think-for-itself-it-turns-to-lobbyists/387295/

95 Kosuke Takeuchi and Yukio Tajima, "Japan to Form Digital Policy Agency Led by Private Sector Figure," *Nikkei Asia,* September 18, 2020, https://asia.nikkei.com/Politics/Japan-to-form-digital-policy-agency-led-by-private-sector-figure?

96 Russell Deeks, "The Digital Silk Road – China's $200 billion project," *Science Focus,* December 8, 2018, https://www.sciencefocus.com/future-technology/the-digital-silk-road-chinas-200-billion-project/

97 Jonathan E. Hillman, "How Big is China's Belt and Road?" Center for Strategic and International Studies, April 3, 2018, https://www.csis.org/analysis/how-big-chinas-belt-and-road

98 Jude Blanchett and Jonathan E. Hillman, "China's Digital Silk Road After the Coronavirus," Center for Strategic and International Studies, April 13, 2020, https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus

99 U.S. International Development Finance Corporation, https://www.dfc.gov/

100 "Digital Economy Report 2019," United Nations Conference on Trade and Development, September 4, 2019, https://unctad.org/system/files/official-document/der2019_overview_en.pdf

101 "Digital Divide Will Worsen Inequalities Without Better Global Cooperation," United Nations News, September 4, 2019, https://news.un.org/en/story/2019/09/1045572

102 "2018 Fact Sheet: Key Barriers to Digital Trade," United States Trade Representative, March 2018, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital

103 Paresh Dave, "China Exports Its Restrictive Internet Policies to Dozens of Countries: Report," *Reuters,* November 1, 2018, https://www.reuters.com/article/us-global-internet-surveillance/china-exports-its-restrictive-internet-policies-to-dozens-of-countries-report-idUSKCN1N63KE

104 "A Concrete Agenda for Transatlantic Cooperation on China," Majority Report, U.S. Senate Committee on Foreign Relations, November 2020, https://www.foreign.senate.gov/imo/media/doc/SFRC%20Majority%20China-Europe%20Report%20FINAL%20(P&G).pdf

105 Juan Pedro Tomás, "Huawei to Capture 28.5% of Global Mobile Base Station Market in 2020," *RCR Wireless News,* August 5, 2020, https://www.rcrwireless.com/20200805/5g/huawei-capture-28-global-mobile-base-station-market-2020

106 "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974," United States Trade Representative, March 22, 2018, https://ustr.gov/sites/default/files/Section%20301%20final.pdf

107 Antonio Varas and Raj Varadarajan, "How Restricting Trade with China Could End U.S. Semiconductor Leadership," Boston Consulting Group, March 9, 2020, https://www.bcg.com/publications/2020/restricting-trade-with-china-could-end-united-states-semiconductor-leadership

108 Kennedy, "Washington's China Policy Has Lost Its Wei," https://www.csis.org/analysis/washingtons-china-policy-has-lost-its-wei

109 Melanie Hart and Kelly Magsamen, "Limit, Leverage, and Compete: A New Strategy on China," Center for American Progress, April 3, 2019, https://www.americanprogress.org/issues/security/reports/2019/04/03/468136/limit-leverage-compete-new-strategy-china/

110 Jay Peters, "Second Judge Says Trump Can't Ban TikTok," *The Verge,* December 7, 2020, https://www.theverge.com/2020/12/7/22160239/tiktok-ban-judge-trump-administration-us-commerce-department.

111 James Andrew Lewis, "Take Me to the Cleaners: Negotiating with China," Center for Strategic and International Studies, July 31, 2020, https://www.csis.org/analysis/take-me-cleaners-negotiating-china

112 Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies," *Foreign Affairs,* November/December 2020, https://www.foreignaffairs.com/articles/unit-

ed-states/2020-10-13/uniting-techno-democracies?mc_cid=bcc8981c73&mc_eid=8555e5617a

113 "UK Seeks Alliance to Avoid Reliance on Chinese Tech: The Times," *Reuters,* May 28, 2020, https://www.reuters.com/article/us-britain-tech-coalition/uk-seeks-alliance-to-avoid-reliance-on-chinese-tech-the-times-idUSKBN2343JW; Sam Fleming, Jim Brunsden and Michael Peel, "EU Proposes Fresh Alliance With U.S. in Face of China Challenge," *Financial Times,* November 29, 2020, https://www.ft.com/content/e8e5cf90-7448-459e-8b9f-6f34f03ab77a

114 Leigh Hartman, "Countries Agree on 5G Security in Prague," *Share America,* May 13, 2019, https://share.america.gov/countries-agree-on-5g-security-in-prague/

115 Jonathan Berr, "WannaCry" Ransomware Attack Losses Could Reach $4 Billion," *CBSNews,* May 16, 2017, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

116 "CEA Report: Cost of Malicious Cyber Activity to the U.S. Economy," Thomson Hine, February 20, 2018, https://www.thompsonhine.com/publications/cea-report-cost-of-malicious-cyber-activity-to-the-us-economy

117 Nathan Bomey and Kevin Johnson, "What You Need to Know About the FireEye Hack: Cybersecurity Attack Against U.S. Government," *USA Today,* December 14, 2020, https://www.usatoday.com/story/tech/2020/12/14/fireeye-solarwinds-hack-breach-cybersecurity-attack/6538645002/

118 Melanie Hart and Jordan Link, "There Is a Solution to the Huawei Challenge," Center for American Progress, October 14, 2020, https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/

119 Dylan Gerstel and Jack Caporal, "Trade Trilateral Targets China's Industrial Subsidies," Center for Strategic and International Studies, January 22, 2020, https://www.csis.org/analysis/trade-trilateral-targets-chinas-industrial-subsidies

120 Jeanne Whalen, "Government Should Take Bigger Role in Promoting U.S. Technology or Risk Losing Ground to China, Commission Says," *Washington Post,* December 1, 2020, https://www.washingtonpost.com/technology/2020/12/01/us-policy-china-technology/

121 Lindsay Gorman, "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything," Alliance for Securing Democracy, October 27, 2020, https://securingdemocracy.gmfus.org/future-internet/

122 Christie Lawrence and Sean Cordey, "The Case for Increased Transatlantic Cooperation on Artificial Intelligence," Belfer Center, Harvard Kennedy School, August 2020, https://www.belfercenter.org/publication/case-increased-transatlantic-cooperation-artificial-intelligence

123 Cohen and Fontaine, "Uniting the Techno-Democracies," https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies?mc_cid=bcc8981c73&mc_eid=8555e5617a

124 "Arrangement on Officially Supported Export Credits," OECD, accessed January 2021, https://www.oecd.org/trade/topics/export-credits/arrangement-and-sector-understandings/

125 "Aid and Export Credits," OECD, accessed January 2021, https://www.oecd.org/trade/topics/export-credits/aid-and-export-credits/

126 Andrew Lipsman, "Global Ecommerce 2019," *Insider Intelligence,* June 27, 2019, https://www.emarketer.com/content/global-ecommerce-2019

127 "76 WTO Partners Launch Talks on E-commerce," European Commission, January 25, 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974

128 Logan Finucan, "USMCA: What's in the Digital Chapter for Your Company," Access Partnership, January 29, 2020, https://www.accesspartnership.com/usmca-whats-in-the-digital-chapter-for-your-company/

129 "Next Steps, a Timeline of New Zealand's Ratification Process, and Details of Negotiation Rounds Are Below," New Zealand Foreign Affairs & Trade, accessed January 2021, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement/next-steps-and-timeline/

130 Wendy Cutler, "Reengaging the Asia-Pacific on Trade: A TPP Roadmap for the Next U.S. Administration," The Asia Society Policy Institute, September 2020, https://asiasociety.org/sites/default/files/2020-09/A%20TPP%20Roadmap%20for%20the%20Next%20U.S.%20Administration.pdf

131 Joshua P. Meltzer, "The United States-Mexico-Canada Agreement: Developing Trade Policy for Digital Trade," *Trade, Law, and Development Vol. 11, No. 2,* Winter 2019, http://www.tradelawdevelopment.com/index.php/tld/article/view/11%282%29%20TL%26D%20239%20%282019%29/365

132 "USTR Announces Initiation of Section 301 Investigation into France's Digital Services Tax," United States Trade Representative, July 10, 2019, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/july/ustr-announces-initiation-section-301

133 "USTR Initiates Section 301 Investigations of Digital Services Taxes," United States Trade Representative, June 2, 2020, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2020/june/ustr-initiates-section-301-investigations-digital-services-taxes

134 Alan Rappeport, Ana Swanson, Jim Tankersley, and Liz Alderman, "U.S. Withdraws from Global Digital Tax Talks," *New York Times,* June 17, 2020, https://www.nytimes.com/2020/06/17/us/politics/us-digital-tax-talks.html

135 Jude Blanchett and Jonathan E. Hillman, "China's Digital Silk Road After the Coronavirus," Center for Strategic and International Studies, April 13, 2020, https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus

AMERICAN
LEADERSHIP
INITIATIVE

www.American-Leadership.org